

# Service Authorization Reference

**Issue** 01  
**Date** 2025-12-11



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

# Contents

- 1 System-defined Policies/Roles..... 1
- 2 System-defined Identity Policies..... 40
- 3 Identity Policy-based Authorization.....58
  - 3.1 Compute.....58
    - 3.1.1 Auto Scaling (AS)..... 58
    - 3.1.2 Bare Metal Server (BMS)..... 74
    - 3.1.3 Elastic Cloud Server (ECS)..... 87
    - 3.1.4 Image Management Service (IMS)..... 108
    - 3.1.5 FunctionGraph..... 118
    - 3.1.6 Cloud Data Center..... 145
  - 3.2 Storage..... 156
    - 3.2.1 Object Storage Service (OBS)..... 156
    - 3.2.2 Cloud Backup and Recovery (CBR)..... 197
    - 3.2.3 Elastic Volume Service (EVS)..... 216
    - 3.2.4 Scalable File Service Turbo (SFS Turbo)..... 229
  - 3.3 Networking..... 246
    - 3.3.1 Enterprise Router..... 246
    - 3.3.2 Virtual Private Cloud..... 260
    - 3.3.3 Elastic IP..... 312
    - 3.3.4 Direct Connect..... 336
    - 3.3.5 VPC Endpoint..... 357
    - 3.3.6 Global accelerator..... 371
    - 3.3.7 NAT Gateway..... 384
    - 3.3.8 Cloud Connect..... 404
    - 3.3.9 Elastic Load Balance..... 439
  - 3.4 Containers..... 460
    - 3.4.1 Cloud Container Engine..... 460
    - 3.4.2 Cloud Container Instance..... 497
    - 3.4.3 SWR Basic Edition..... 512
    - 3.4.4 SWR Enterprise Edition..... 529
  - 3.5 Content Delivery & Edge Computing.....564
    - 3.5.1 Content Delivery Network (CDN)..... 564

|                                                                     |      |
|---------------------------------------------------------------------|------|
| 3.5.2 CloudPond.....                                                | 574  |
| 3.6 Databases.....                                                  | 580  |
| 3.6.1 Relational Database Service (RDS).....                        | 580  |
| 3.6.2 GaussDB.....                                                  | 621  |
| 3.6.3 Document Database Service (DDS).....                          | 642  |
| 3.6.4 Data Replication Service (DRS).....                           | 664  |
| 3.6.5 TaurusDB.....                                                 | 724  |
| 3.6.6 DAS.....                                                      | 766  |
| 3.7 Security & Compliance.....                                      | 780  |
| 3.7.1 Data Encryption Workshop (DEW).....                           | 780  |
| 3.7.1.1 Key Management Service (KMS).....                           | 780  |
| 3.7.1.2 Key Pair Service (KPS).....                                 | 813  |
| 3.7.1.3 Cloud Secret Management Service (CSMS).....                 | 822  |
| 3.7.2 Anti-DDoS Service (AAD).....                                  | 834  |
| 3.7.2.1 Cloud Native Anti-DDoS Basic.....                           | 834  |
| 3.7.2.2 Cloud Native Anti-DDoS Advanced.....                        | 841  |
| 3.7.2.3 Advanced Anti-DDoS.....                                     | 850  |
| 3.7.3 Cloud Firewall (CFW).....                                     | 864  |
| 3.7.4 Cloud Bastion Host (CBH).....                                 | 897  |
| 3.7.5 Cloud Certificate & Manager (CCM).....                        | 907  |
| 3.7.6 Database Security Service (DBSS).....                         | 918  |
| 3.7.7 Data Security Center (DSC).....                               | 956  |
| 3.7.8 Web Application Firewall (WAF).....                           | 967  |
| 3.7.9 Host Security Service (HSS).....                              | 994  |
| 3.7.10 SecMaster.....                                               | 1137 |
| 3.8 AI.....                                                         | 1197 |
| 3.8.1 ModelArts.....                                                | 1197 |
| 3.9 Analytics.....                                                  | 1231 |
| 3.9.1 Cloud Search Service (CSS).....                               | 1231 |
| 3.9.2 Actions Supported by Identity Policy-based Authorization..... | 1265 |
| 3.9.3 Data Lake Insight(DLI).....                                   | 1276 |
| 3.9.4 MapReduce Service (MRS).....                                  | 1300 |
| 3.9.5 Data Warehouse Service (DWS).....                             | 1305 |
| 3.10 Middleware.....                                                | 1386 |
| 3.10.1 Cloud Service Engine CSE.....                                | 1386 |
| 3.10.2 Distributed Message Service for Kafka (Kafka).....           | 1395 |
| 3.10.3 Distributed Message Service for RabbitMQ (RabbitMQ).....     | 1414 |
| 3.10.4 Distributed Message Service for RocketMQ (RocketMQ).....     | 1422 |
| 3.10.5 API Gateway (APIG).....                                      | 1437 |
| 3.10.6 Distributed Cache Service (DCS).....                         | 1497 |
| 3.11 Developer Services.....                                        | 1522 |
| 3.11.1 ServiceStage.....                                            | 1522 |



|                                                                       |      |
|-----------------------------------------------------------------------|------|
| 3.11.2 CodeArts.....                                                  | 1546 |
| 3.11.3 CodeArts Pipeline.....                                         | 1558 |
| 3.11.4 Cloud Application Engine.....                                  | 1561 |
| 3.12 Business Applications.....                                       | 1578 |
| 3.12.1 Domain Name Service.....                                       | 1578 |
| 3.13 Media Services.....                                              | 1601 |
| 3.13.1 Live (Live).....                                               | 1601 |
| 3.13.2 Media Processing Center (MPC).....                             | 1615 |
| 3.14 Management & Governance.....                                     | 1626 |
| 3.14.1 Identity and Access Management (IAM).....                      | 1626 |
| 3.14.2 Organizations.....                                             | 1668 |
| 3.14.3 Resource Access Manager (RAM).....                             | 1685 |
| 3.14.4 IAM Identity Center.....                                       | 1698 |
| 3.14.5 Resource Management Service (RMS).....                         | 1735 |
| 3.14.6 Tag Management Service (TMS).....                              | 1764 |
| 3.14.7 Enterprise Project Management Service (EPS).....               | 1767 |
| 3.14.8 Cloud Eye.....                                                 | 1771 |
| 3.14.9 Simple Message Notification (SMN).....                         | 1822 |
| 3.14.10 Log Tank Service (LTS).....                                   | 1840 |
| 3.14.11 Actions Supported by Identity Policy-based Authorization..... | 1880 |
| 3.14.12 Resource Formation Service (RFS).....                         | 1887 |
| 3.14.13 Security Token Service (STS).....                             | 1898 |
| 3.14.14 IAM Access Analyzer (IAA).....                                | 1903 |
| 3.14.15 Resource Governance Center (RGC).....                         | 1913 |
| 3.14.16 Cloud Operations Center (COC).....                            | 1928 |
| 3.14.17 Application Performance Management (APM).....                 | 2015 |
| 3.14.18 Application Operations Management.....                        | 2026 |
| 3.14.19 Optimization Advisor.....                                     | 2037 |
| 3.15 Migration.....                                                   | 2052 |
| 3.15.1 Object Storage Migration Service (OMS).....                    | 2052 |
| 3.15.2 Server Migration Service (SMS).....                            | 2059 |
| 3.16 Customer Services.....                                           | 2070 |
| 3.16.1 Billing Center.....                                            | 2070 |
| 3.16.2 Cost Center.....                                               | 2075 |
| 3.16.3 My Account.....                                                | 2082 |
| 3.16.4 Enterprise Center.....                                         | 2084 |
| 3.16.5 Customer Operation Capabilities.....                           | 2088 |

# 1 System-defined Policies/Roles

New IAM users do not have any permissions assigned by default. You need to first **add them to one or more groups**, and then **attach policies or roles to these groups** on the old IAM console. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

**Scope:** The projects for which permissions granted to a user group will be applied.

- Global services: Services deployed without specifying physical regions, such as Object Storage Service (OBS) and Content Delivery Network (CDN), are called global services. Permissions for these services must be assigned globally.
- Region-specific projects: Services deployed in specific regions, such as Elastic Cloud Server (ECS) and Bare Metal Server (BMS), are called project-level services. Permissions for these services must be assigned in region-specific projects and will be applied only for specific regions.
- All resources: Permissions will be applied for both global services and all region-specific projects, including projects created later.

**Type:** You can assign users permissions by using roles and policies. Policies are a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. For details, see **Permissions**.

- For services that provide both roles and policies, preferentially use policies to assign permissions.
- For services that support policy-based access control, you can **create custom policies** to supplement system-defined policies to allow or deny access to specific types of resources under certain conditions.

## BASE

| Service | Scope           | Policy/<br>Role<br>Name | Type   | Description                                                                |
|---------|-----------------|-------------------------|--------|----------------------------------------------------------------------------|
| BASE    | Global services | FullAccess              | Policy | Full permissions for all services that support policy-based authorization. |

| Service | Scope           | Policy/<br>Role<br>Name | Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------|-----------------|-------------------------|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | All resources   | Tenant Guest            | Role | Read-only permissions for all services except IAM.<br><b>NOTE</b> <ul style="list-style-type: none"> <li>If the permission scope is <b>Global services</b>, they will be applied for global services.</li> <li>If the permission scope is <b>All resources</b>, they will be applied for both global services and all region-specific projects, including projects created later.</li> <li>If the permission scope is <b>Region-specific projects</b>, they will be applied only for specific projects.</li> </ul> |
|         | All resources   | Tenant Administrator    |      | Full permissions for all services except IAM.<br><b>NOTE</b> <ul style="list-style-type: none"> <li>If the permission scope is <b>Global services</b>, they will be applied for global services.</li> <li>If the permission scope is <b>All resources</b>, they will be applied for both global services and all region-specific projects, including projects created later.</li> <li>If the permission scope is <b>Region-specific projects</b>, they will be applied only for specific projects.</li> </ul>      |
|         | Global services | Agent Operator          |      | Permissions for switching roles to access resources of delegating accounts.                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Compute

| Service                                               | Scope                    | Policy/<br>Role<br>Name     | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|--------------------------|-----------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Elastic Cloud Server (ECS)<br>(Project-level service) | Region-specific projects | ECS FullAccess              | Policy | Full permissions for ECS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                       |                          | ECS ReadOnly Access         |        | Read-only permissions for ECS.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                       |                          | ECS CommonOperations        |        | Permissions for starting, stopping, restarting, and querying ECSs.                                                                                                                                                                                                                                                                                                                                                                                                                         |
|                                                       |                          | Server Administrator        | Role   | <p>Full permissions for ECS. This role must be used together with the <b>Tenant Guest</b> role in the same project.</p> <p>If a user needs to create, delete, or change resources of other services, the user must also be granted <b>administrator permissions</b> of the corresponding services in the same project.</p> <p>For example, if a user needs to create a new VPC when creating an ECS, the user must also be granted permissions with the <b>VPC Administrator</b> role.</p> |
| Bare Metal Server (BMS)<br>(Project-level service)    | Region-specific projects | BMS FullAccess              | Policy | Full permissions for BMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                                       |                          | BMS ReadOnly Access         |        | Read-only permissions for BMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                       |                          | BMS CommonOperations        |        | Permissions for starting, stopping, restarting, and querying BMSs.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Auto Scaling (AS)<br>(Project-level service)          | Region-specific projects | AutoScaling FullAccess      | Policy | Full permissions for the Auto Scaling service.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                       |                          | AutoScaling ReadOnly Access |        | Read-only permissions for AS.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Service                                                | Scope                    | Policy/<br>Role<br>Name        | Type   | Description                                                                                                                                                                                                                           |
|--------------------------------------------------------|--------------------------|--------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                        |                          | AutoScaling Administrator      | Role   | Full permissions for all AS resources.<br><br>This role must be used together with the <b>ELB Administrator</b> , <b>CES Administrator</b> , <b>Server Administrator</b> , and <b>Tenant Administrator</b> roles in the same project. |
| Image Management Service (IMS) (Project-level service) | Region-specific projects | IMS FullAccess                 | Policy | Full permissions for IMS.                                                                                                                                                                                                             |
|                                                        |                          | IMS ReadOnly Access            |        | Read-only permissions for IMS.                                                                                                                                                                                                        |
|                                                        |                          | IMS Administrator              | Role   | Full permissions for IMS.<br><br>This role must be used together with the <b>Tenant Administrator</b> role.                                                                                                                           |
|                                                        |                          | Server Administrator           |        | Permissions for creating, deleting, querying, modifying, and uploading images. This role must be used together with the <b>IMS Administrator</b> role in the same project.                                                            |
| FunctionGraph (Project-level service)                  | Region-specific projects | FunctionGraph FullAccess       | Policy | Full permissions for FunctionGraph.                                                                                                                                                                                                   |
|                                                        |                          | FunctionGraph ReadOnly Access  |        | Read-only permissions for FunctionGraph.                                                                                                                                                                                              |
|                                                        |                          | FunctionGraph CommonOperations |        | Common operation permissions for FunctionGraph, including permissions for querying functions and triggers and invoking functions.                                                                                                     |
|                                                        |                          | FunctionGraph Administrator    | Role   | Permissions for managing FunctionGraph functions and triggers.<br><br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                                                                          |

| Service                                           | Scope                    | Policy/<br>Role<br>Name  | Type   | Description                                                                      |
|---------------------------------------------------|--------------------------|--------------------------|--------|----------------------------------------------------------------------------------|
|                                                   |                          | FunctionGraph<br>Invoker |        | Permissions for querying FunctionGraph functions and triggers.                   |
| Cloud Phone Host (CPH)<br>(Project-level service) | Region-specific projects | CPH Administrator        | Role   | Full permissions for CPH.                                                        |
|                                                   |                          | CPH User                 |        | Read-only permissions for CPH.                                                   |
| Dedicated Host (DeH)<br>(Project-level service)   | Region-specific projects | DeH FullAccess           | Policy | Full permissions for DeH.                                                        |
|                                                   |                          | DeH CommonOperations     |        | Basic operation permissions for DeH.                                             |
|                                                   |                          | DeH ReadOnly Access      |        | Read-only permissions for DeH. Users with these permissions can only query DeHs. |

## Storage

| Service                                          | Scope           | Policy/Role<br>Name | Type   | Description                                                                                                                                                                                                                    |
|--------------------------------------------------|-----------------|---------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Global service)<br>Object Storage Service (OBS) | Global services | OBS OperateAccess   | Policy | Users with this permission can perform all operations specified by <b>OBS ReadOnlyAccess</b> and perform basic object operations, such as uploading objects, downloading objects, deleting objects, and obtaining object ACLs. |
|                                                  |                 | OBS ReadOnlyAccess  |        | Users with this permission can list buckets, obtain basic bucket information, obtain bucket metadata, and list objects.                                                                                                        |
|                                                  |                 | OBS Buckets Viewer  | Role   | Users with this permission can list buckets, obtain basic bucket information, and obtain bucket metadata.                                                                                                                      |

| Service                                                    | Scope                    | Policy/Role Name               | Type   | Description                                                                                                                                                |
|------------------------------------------------------------|--------------------------|--------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Elastic Volume Service (EVS)<br>(Project-level service)    | Region-specific projects | EVS FullAccess                 | Policy | Full permissions for EVS. Users granted these permissions can create, mount, uninstall, query, and delete EVS resources, and expand capacity of EVS disks. |
|                                                            |                          | EVS ReadOnlyAccess             |        | Read-only permissions for EVS. Users granted these permissions can view EVS resource data only.                                                            |
|                                                            |                          | Server Administrator           | Role   | Full permissions for EVS.                                                                                                                                  |
| Cloud Backup and Recovery (CBR)<br>(Project-level service) | Region-specific projects | CBR FullAccess                 | Policy | Administrator permissions for using all vaults and policies on CBR.                                                                                        |
|                                                            |                          | CBR BackupsAndVaultsFullAccess |        | Common user permissions for creating, viewing, and deleting vaults on CBR.                                                                                 |
|                                                            |                          | CBR ReadOnlyAccess             |        | Read-only permissions for viewing data on CBR.                                                                                                             |
| Content Delivery Network (CDN)<br>(Global service)         | Global services          | CDN DomainReadOnlyAccess       | Policy | Read-only permissions for CDN acceleration domain names.                                                                                                   |
|                                                            |                          | CDN StatisticsReadOnlyAccess   |        | Read-only permissions for CDN statistics.                                                                                                                  |
|                                                            |                          | CDN LogsReadOnlyAccess         |        | Read-only permissions for CDN logs.                                                                                                                        |
|                                                            |                          |                                |        |                                                                                                                                                            |
|                                                            |                          | CDN RefreshAndPreheatAccess    |        | Permissions for cache refreshing and preheating.                                                                                                           |
|                                                            |                          | CDN Administrator              | Role   | Full permissions for CDN.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                                        |

| Service                                                       | Scope                    | Policy/Role Name         | Type   | Description                                                                                                                                          |
|---------------------------------------------------------------|--------------------------|--------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| CloudPond<br>(Global service)                                 | Global services          | IES FullAccess           | Policy | Administrator permissions for CloudPond. Users with these permissions can perform all operations on CloudPond.                                       |
|                                                               |                          | IES ReadOnlyAccess       | Policy | Read-only permissions for CloudPond. Users with these permissions can only view CloudPond data.                                                      |
| Business Recovery Service (BRS)<br>(Project-level service)    | Region-specific projects | SDRS Administrator       | Role   | Full permissions for BRS.<br>This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project. |
| Scalable File Service (SFS)<br>(Project-level service)        | Region-specific projects | SFS FullAccess           | Policy | Full permissions for SFS.                                                                                                                            |
|                                                               |                          | SFS ReadOnlyAccess       |        | Read-only permissions for SFS.                                                                                                                       |
|                                                               |                          | SFS Turbo FullAccess     |        | Full permissions for SFS Turbo.                                                                                                                      |
|                                                               |                          | SFS Turbo ReadOnlyAccess |        | Read-only permissions for SFS Turbo.                                                                                                                 |
|                                                               |                          | SFS Administrator        | Role   | Full permissions for SFS.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                                  |
| Cloud Server Backup Service (CSBS)<br>(Project-level service) | Region-specific projects | CSBS Administrator       | Role   | Full permissions for CSBS.<br>This role must be used together with the <b>Server Administrator</b> role in the same project.                         |



| Service                                                | Scope                    | Policy/Role Name  | Type | Description                                                                                                                                          |
|--------------------------------------------------------|--------------------------|-------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Volume Backup Service (VBS)<br>(Project-level service) | Region-specific projects | VBS Administrator | Role | Full permissions for VBS.<br>This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project. |

## Network

| Service                                                | Scope                    | Policy/Role Name     | Type   | Description                                                                                                                                                                                                                   |
|--------------------------------------------------------|--------------------------|----------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Private Cloud (VPC)<br>(Project-level service) | Region-specific projects | VPC FullAccess       | Policy | Full permissions for VPC.                                                                                                                                                                                                     |
|                                                        |                          | VPC ReadOnlyAccess   |        | Read-only permissions for VPC.                                                                                                                                                                                                |
|                                                        |                          | VPC Administrator    | Role   | Permissions for VPC, excluding permissions for creating, modifying, deleting, and viewing security groups and security group rules.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project. |
|                                                        |                          | Server Administrator |        | Permissions for performing operations on EIPs, security groups, and ports.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                                                          |
| Elastic Load Balance (ELB)<br>(Project-level service)  | Region-specific projects | ELB FullAccess       | Policy | Full permissions for ELB.                                                                                                                                                                                                     |
|                                                        |                          | ELB ReadOnlyAccess   |        | Read-only permissions for ELB.                                                                                                                                                                                                |
|                                                        |                          | ELB Administrator    | Role   | Full permissions for ELB.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                                                                                                           |

| Service                                                  | Scope                    | Policy/Role Name             | Type   | Description                                                                                                                                                |
|----------------------------------------------------------|--------------------------|------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NAT Gateway<br>(Project-level service)                   | Region-specific projects | NAT FullAccess               | Policy | Full permissions for NAT Gateway.                                                                                                                          |
|                                                          |                          | NAT ReadOnlyAccess           |        | Read-only permissions for NAT Gateway.                                                                                                                     |
|                                                          |                          | NAT Administrator            | Role   | Full permissions for NAT Gateway.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                                |
| Direct Connect<br>(Project-level service)                | Region-specific projects | Direct Connect Administrator | Role   | Full permissions for Direct Connect.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                             |
|                                                          |                          | DCaaS Partner                |        | Direct Connect partner with permissions for creating hosted and standard connections for other users.                                                      |
|                                                          |                          | DCAAS FullAccess             | Policy | Full permissions for Direct Connect.                                                                                                                       |
|                                                          |                          | DCAAS ReadOnlyAccess         |        | Read-only permissions for Direct Connect.                                                                                                                  |
| Virtual Private Network (VPN)<br>(Project-level service) | Region-specific projects | VPN Administrator            | Role   | Administrator permissions for VPN.<br>This role must be used together with the <b>Tenant Guest</b> and <b>VPC Administrator</b> roles in the same project. |
|                                                          |                          | VPN FullAccess               | Policy | Full permissions for VPN.                                                                                                                                  |
|                                                          |                          | VPN ReadOnlyAccess           |        | Read-only permissions for VPN.                                                                                                                             |

| Service                                              | Scope                    | Policy/Role Name              | Type   | Description                                                                                                                                                                              |
|------------------------------------------------------|--------------------------|-------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name Service (DNS)<br>(Project-level service) | Region-specific projects | DNS Administrator             | Role   | Full permissions for DNS.<br>This role must be used together with the <b>Tenant Guest</b> and <b>VPC Administrator</b> roles in the same project.                                        |
|                                                      |                          | DNS FullAccess                | Policy | Full permissions for DNS.                                                                                                                                                                |
|                                                      |                          | DNS ReadOnlyAccess            |        | Read-only permissions for DNS. Users granted these permissions can only view DNS resources.                                                                                              |
| VPC Endpoint (VPCEP)<br>(Project-level service)      | Region-specific projects | VPCEndpoint Administrator     | Role   | Full permissions for VPCEP.<br>This role must be used together with the <b>Server Administrator</b> , <b>VPC Administrator</b> , and <b>DNS Administrator</b> roles in the same project. |
| Cloud Connect (CC)<br>(Global service)               | Global services          | Cross Connect Administrator   | Role   | CC administrator with full permissions.<br>This role must be used together with the <b>Tenant Guest</b> and <b>VPC Administrator</b> roles in the same project.                          |
|                                                      |                          | CC FullAccess                 | Policy | Full permissions for CC.                                                                                                                                                                 |
|                                                      |                          | CC ReadOnlyAccess             |        | Read-only permissions for CC.                                                                                                                                                            |
|                                                      |                          | CC Network Depend QueryAccess |        | Read-only permissions required to access dependency resources when using CC.                                                                                                             |
| Enterprise Router<br>(Project-level service)         | Region-specific projects | ER FullAccess                 | Policy | Full permissions for ER.                                                                                                                                                                 |
|                                                      |                          | ER ReadOnlyAccess             |        | Read-only permissions for ER.                                                                                                                                                            |

## Containers

| Service                                                   | Scope                    | Policy/Role Name     | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|--------------------------|----------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Container Engine (CCE)<br>(Project-level service)   | Region-specific projects | CCE FullAccess       | Policy | Full permissions for CCE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                                           |                          | CCE ReadOnlyAccess   |        | Permissions to view CCE cluster resources, excluding namespace-level permissions for clusters that have Kubernetes RBAC enabled.                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                                           |                          | CCE Administrator    | Role   | <p>Read and write permissions for CCE clusters and all resources (including workloads and services) in the clusters.</p> <p>This role depends on the following permissions:</p> <p>Global services: <b>OBS Buckets Viewer</b>.</p> <p>Region-specific projects (same projects): <b>Tenant Guest, Server Administrator, ELB Administrator, SFS Administrator, SWR Admin, and APM FullAccess</b>.</p> <p><b>NOTE</b><br/>Users also granted permissions with the <b>NAT Gateway Administrator</b> role can use NAT Gateway functions for clusters.</p> |
| Cloud Container Instance (CCI)<br>(Project-level service) | Region-specific projects | CCI FullAccess       | Policy | Full permissions for CCI. Users granted these permissions can create, delete, query, and update all CCI resources.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                                                           |                          | CCI ReadOnlyAccess   |        | Read-only permissions for CCI. Users granted these permissions can only view CCI resources.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                                           |                          | CCI CommonOperations |        | Common user permissions for CCI. Users granted these permissions can perform all operations except creating, deleting, and modifying role-based access control (RBAC) policies, networks, and namespaced resources.                                                                                                                                                                                                                                                                                                                                  |

| Service                                                         | Scope                    | Policy/Role Name     | Type   | Description                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------|--------------------------|----------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                 |                          | CCI Administrator    | Role   | Administrator permissions for CCI. Users granted these permissions can create, delete, query, and update all CCI resources.                                                                                                                            |
| Software Repository for Container (SWR) (Project-level service) | Region-specific projects | SWR Admin            | Role   | Full permissions for SWR.                                                                                                                                                                                                                              |
|                                                                 |                          | SWR FullAccess       | Policy | Full permissions for SWR enterprise edition.                                                                                                                                                                                                           |
|                                                                 |                          | SWR ReadOnlyAccess   |        | Read-only permissions for SWR enterprise edition. Users with these permissions can query artifact repositories and charts, create temporary credentials, and download artifacts.                                                                       |
|                                                                 |                          | SWR OperateAccess    |        | Operation permissions for SWR enterprise edition. Users with these permissions can query enterprise edition instances, perform operations on artifact repositories and organizations, create temporary credentials, and upload and download artifacts. |
| Gene Container Service (GCS) (Project-level service)            | Region-specific projects | GCS Administrator    | Role   | GCS administrator.                                                                                                                                                                                                                                     |
|                                                                 |                          | GCS FullAccess       | Policy | Full permissions for GCS.                                                                                                                                                                                                                              |
|                                                                 |                          | GCS ReadOnlyAccess   |        | Read-only permissions for GCS.                                                                                                                                                                                                                         |
|                                                                 |                          | GCS CommonOperations |        | Common operation permissions for GCS.                                                                                                                                                                                                                  |
| Application Orchestration Service (AOS) (Project-level service) | Region-specific projects | CDE Admin            | Role   | AOS administrator with full permissions.                                                                                                                                                                                                               |
|                                                                 |                          | CDE Developer        |        | AOS developer.                                                                                                                                                                                                                                         |
|                                                                 |                          | RF FullAccess        | Policy | Full permissions for RF.                                                                                                                                                                                                                               |
|                                                                 |                          | RF ReadOnlyAccess    |        | Read-only permissions for RF.                                                                                                                                                                                                                          |

| Service                                                | Scope           | Policy/Role Name                   | Type   | Description                                                                                     |
|--------------------------------------------------------|-----------------|------------------------------------|--------|-------------------------------------------------------------------------------------------------|
|                                                        |                 | RF DeployByExecutionPlanOperations |        | Create, execute, and read permissions for execution plans and read permissions for stacks.      |
| Ubiquitous Cloud Native Service (UCS) (Global service) | Global services | UCS FullAccess                     | Policy | UCS administrator permissions, including creating permissions policies and security policies.   |
|                                                        |                 | UCS CommonOperations               |        | Common UCS user permissions for creating workloads, distributing traffic, and other operations. |
|                                                        |                 | UCS CIAOperations                  |        | UCS Container Intelligent Analysis (CIA) administrator with full permissions.                   |
|                                                        |                 | UCS ReadOnlyAccess                 |        | Read-only permissions (excluding CIA) for UCS.                                                  |

## Security & Compliance

| Service                                          | Scope                    | Policy/Role Name        | Type   | Description                                                                                                            |
|--------------------------------------------------|--------------------------|-------------------------|--------|------------------------------------------------------------------------------------------------------------------------|
| Anti-DDoS (Project-level service)                | Region-specific projects | Anti-DDoS Administrator | Role   | Full permissions for Anti-DDoS. This role must be used together with the <b>Tenant Guest</b> role in the same project. |
| Advanced Anti-DDoS (AAD) (Project-level service) | Region-specific projects | CAD Administrator       | Role   | AAD administrator with full permissions.                                                                               |
| Cloud Native Anti-DDoS (CNAD) (Global service)   | Global services          | CNAD FullAccess         | Policy | Full permissions for Cloud Native Anti-DDoS (CNAD).                                                                    |
|                                                  |                          | CNAD ReadOnlyAccess     |        | Read-only permissions for CNAD.                                                                                        |

| Service                                                     | Scope                    | Policy/Role Name            | Type   | Description                                                                                                                      |
|-------------------------------------------------------------|--------------------------|-----------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------|
| Vulnerability Scan Service (VSS)<br>(Project-level service) | Region-specific projects | VSS ReadOnlyAccess          | Role   | Read-only permissions for VSS.                                                                                                   |
| Host Security Service (HSS)<br>(Project-level service)      | Region-specific projects | HSS Administrator           | Role   | Full permissions for HSS.                                                                                                        |
|                                                             |                          | HSS FullAccess              | Policy | Full permissions for HSS.                                                                                                        |
|                                                             |                          | HSS ReadOnlyAccess          |        | Read-only permissions for HSS.                                                                                                   |
| Database Security Service (DBSS)<br>(Project-level service) | Region-specific projects | DBSS System Administrator   | Role   | Full permissions for DBSS.                                                                                                       |
|                                                             |                          | DBSS Audit Administrator    |        | Security auditing permissions for DBSS.                                                                                          |
|                                                             |                          | DBSS Security Administrator |        | Security protection permissions for DBSS.                                                                                        |
|                                                             |                          | DBSS FullAccess             | Policy | Full permissions for DBSS.                                                                                                       |
|                                                             |                          | DBSS ReadOnlyAccess         |        | Read-only permissions for DBSS. Users granted these permissions can only view this service and cannot configure resources in it. |
| Data Encryption Workshop (DEW)<br>(Project-level service)   | Region-specific projects | KMS Administrator           | Role   | Administrator permissions for DEW encryption keys.                                                                               |
|                                                             |                          | KMS CMKFullAccess           | Policy | All permissions for DEW encryption keys.                                                                                         |

| Service                                                   | Scope                    | Policy/Role Name          | Type   | Description                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|--------------------------|---------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                           |                          | DEW KeypairFullAccess     |        | All permissions for DEW key pairs.                                                                                                                                                                                                                   |
|                                                           |                          | DEW KeypairReadOnlyAccess |        | Read-only permissions for DEW key pairs.                                                                                                                                                                                                             |
|                                                           |                          | CSMS FullAccess           |        | Full permissions for Cloud Secret Management Service (CSMS).                                                                                                                                                                                         |
|                                                           |                          | CSMS ReadOnlyAccess       |        | Read-only permissions for CSMS.                                                                                                                                                                                                                      |
| Web Application Firewall (WAF)<br>(Project-level service) | Region-specific projects | WAF Administrator         | Role   | Full permissions for WAF.<br>This role must be used together with the <b>Tenant Guest</b> role in the global service project and with the <b>Server Administrator</b> role in the same project.                                                      |
|                                                           |                          | WAF FullAccess            | Policy | Full permissions for WAF.                                                                                                                                                                                                                            |
|                                                           |                          | WAF ReadOnlyAccess        |        | Read-only permissions for WAF.                                                                                                                                                                                                                       |
| Cloud Firewall (CFW)<br>(Project-level service)           | Region-specific projects | CFW FullAccess            | Policy | Full permissions for CFW.                                                                                                                                                                                                                            |
|                                                           |                          | CFW ReadOnlyAccess        |        | Read-only permissions for CFW.                                                                                                                                                                                                                       |
| Cloud Certificate & Manager (CCM)<br>(Global service)     | Global services          | SCM Administrator         | Policy | SCM administrator permissions. Users with SCM administrator permissions have all the permissions for the SCM service.<br><br>This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project. |
|                                                           |                          | SCM FullAccess            |        | Full permissions for SCM.                                                                                                                                                                                                                            |



| Service                                                             | Scope                    | Policy/Role Name               | Type   | Description                                                                                                                                                               |
|---------------------------------------------------------------------|--------------------------|--------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     |                          | SCM<br>ReadOnlyAccess          |        | Read-only permissions for SCM. Users with these permissions can only query certificates but cannot add, delete, or modify certificates.                                   |
|                                                                     |                          | PCA<br>FullAccess              |        | All permissions for PCA.                                                                                                                                                  |
| Cloud Bastion Host (CBH)<br>(Project-level service)                 | Region-specific projects | CBH<br>FullAccess              | Policy | Full permissions for CBH instances.                                                                                                                                       |
|                                                                     |                          | CBH<br>ReadOnlyAccess          |        | Read-only permissions for CBH instances. Users who have read-only permissions granted can only view CBH instances but cannot configure or perform operations on services. |
| Data Security Center (DSC)<br>(Project-level service)               | Region-specific projects | DSC<br>FullAccess              | Policy | Full permissions for DSC.                                                                                                                                                 |
|                                                                     |                          | DSC<br>ReadOnlyAccess          |        | Read-only permissions for DSC.                                                                                                                                            |
|                                                                     |                          | DSC<br>DashboardReadOnlyAccess |        | Read-only permissions for the overview page of DSC.                                                                                                                       |
| Database and Application Migration (UGO)<br>(Project-level service) | Region-specific projects | UGO<br>FullAccess              | Policy | Full permissions for UGO.                                                                                                                                                 |
|                                                                     |                          | UGO<br>ReadOnlyAccess          |        | Read-only permissions for UGO.                                                                                                                                            |
|                                                                     |                          | UGO<br>CommonOperations        |        | SQL statement conversion permission for UGO.                                                                                                                              |

## Management & Governance

| Service                                                            | Scope                    | Policy/Role Name       | Type   | Description                                                                                                                                                                                                                                |
|--------------------------------------------------------------------|--------------------------|------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identity and Access Management (IAM)<br>(Global service)           | Global services          | IAM ReadOnlyAccess     | Policy | Read-only permissions for IAM.                                                                                                                                                                                                             |
|                                                                    | Global services          | Security Administrator | Role   | All permissions (excluding switching roles) for IAM.                                                                                                                                                                                       |
| Cloud Eye<br>(Project-level service)                               | Region-specific projects | CES Administrator      | Role   | Full permissions for Cloud Eye. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project.                                                                                    |
|                                                                    | Region-specific projects | CES FullAccess         | Policy | Administrator permissions for performing all operations on Cloud Eye.<br><br>The monitoring function of Cloud Eye involves the query of cloud resources, which requires the relevant cloud services to support policy-based authorization. |
|                                                                    | Region-specific projects | CES ReadOnlyAccess     |        | Read-only permissions for viewing data on Cloud Eye.<br><br>The monitoring function of Cloud Eye involves the query of cloud resources, which requires the relevant cloud services to support policy-based authorization.                  |
| Application Operations Management (AOM)<br>(Project-level service) | Region-specific projects | AOM FullAccess         | Policy | Full permissions for AOM.                                                                                                                                                                                                                  |
|                                                                    |                          | AOM ReadOnlyAccess     |        | Read-only permissions for AOM.                                                                                                                                                                                                             |

| Service                                                             | Scope                    | Policy/Role Name   | Type   | Description                                                                                                                                                                      |
|---------------------------------------------------------------------|--------------------------|--------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Performance Management (APM)<br>(Project-level service) | Region-specific projects | APM FullAccess     | Policy | Full permissions for APM.                                                                                                                                                        |
|                                                                     |                          | APM ReadOnlyAccess |        | Read-only permissions for APM.                                                                                                                                                   |
|                                                                     |                          | APM Administrator  | Role   | Full permissions for APM.                                                                                                                                                        |
| Cloud Trace Service (CTS)<br>(Project-level service)                | Region-specific projects | CTS FullAccess     | Policy | Full permissions for CTS.<br><b>NOTE</b><br>To enable CTS, a user must be granted permissions using the <b>CTS FullAccess</b> policy and the <b>Security Administrator</b> role. |
|                                                                     |                          | CTS ReadOnlyAccess |        | Read-only permissions for CTS.                                                                                                                                                   |
|                                                                     |                          | CTS Administrator  | Role   | Full permissions for CTS.<br>This role must be used together with the <b>Tenant Guest</b> and <b>Tenant Administrator</b> roles in the same project.                             |
| Log Tank Service (LTS)<br>(Project-level service)                   | Region-specific projects | LTS FullAccess     | Policy | Full permissions for LTS.                                                                                                                                                        |
|                                                                     |                          | LTS ReadOnlyAccess |        | Read-only permissions for LTS.                                                                                                                                                   |
|                                                                     |                          | LTS Administrator  | Role   | Full permissions for LTS.<br>This role must be used together with the <b>Tenant Guest</b> and <b>Tenant Administrator</b> roles in the same project.                             |
| Tag Management Service (TMS)<br>(Global service)                    | Global services          | TMS FullAccess     | Policy | Full permissions for TMS.                                                                                                                                                        |
|                                                                     |                          | TMS ReadOnlyAccess |        | Read-only permissions for TMS.                                                                                                                                                   |

| Service | Scope | Policy/Role Name  | Type | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|-------|-------------------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |       | TMS Administrator | Role | <p>Administrator permissions for TMS.</p> <p>The permissions depend on the following policies:</p> <ul style="list-style-type: none"> <li>• <b>Tenant Guest:</b> a global or project-level policy, which must be assigned in the same project as <b>TMS Administrator</b>.</li> <li>• <b>Server Administrator:</b> a project-level policy, which must be assigned in the same project as <b>TMS Administrator</b>.</li> <li>• <b>Tenant Guest:</b> a global policy. Select <b>Global services</b> for <b>Scope</b>.</li> <li>• <b>Tenant Administrator:</b> a global policy. Select <b>Global services</b> for <b>Scope</b>.</li> <li>• <b>IMS Administrator:</b> a project-level policy, which must be assigned in the same project as <b>TMS Administrator</b>.</li> <li>• <b>AutoScaling Administrator:</b> a project-level policy, which must be assigned in the same project as <b>TMS Administrator</b>.</li> <li>• <b>VPC Administrator:</b> a project-level policy, which must be assigned in the same project as <b>TMS Administrator</b>.</li> <li>• <b>VBS Administrator:</b> a project-level policy, which must be assigned in the same project as <b>TMS Administrator</b>.</li> </ul> |

| Service                                                    | Scope                    | Policy/Role Name                   | Type   | Description                                                                                                                                                                              |
|------------------------------------------------------------|--------------------------|------------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Resource Template Service (RTS)<br>(Project-level service) | Region-specific projects | RTS Administrator                  | Role   | Full permissions for RTS. This role must be used together with the <b>Server Administrator</b> , <b>ELB Administrator</b> , and <b>CES Administrator</b> roles in the same project.      |
| OneAccess<br>(Global service)                              | Global services          | OneAccess FullAccess               | Policy | Full permissions for OneAccess, including permissions for creating a custom domain name and modifying the domain name certificate. IAM users cannot purchase or use OneAccess instances. |
|                                                            |                          | OneAccess ReadOnlyAccess           |        | Read-only permissions for OneAccess. Users granted these permissions can only view this service and cannot configure resources in it.                                                    |
| Config<br>(Global service)                                 | Global services          | Config ConsoleFullAccess           | Policy | Permissions for all operations on the Config console.                                                                                                                                    |
|                                                            |                          | Config FullAccess                  |        | Full permissions for Config.                                                                                                                                                             |
|                                                            |                          | Config ReadOnlyAccess              |        | Read-only permissions for Config.                                                                                                                                                        |
| Resource Access Manager (RAM)<br>(Global service)          | Global services          | RAM FullAccess                     | Policy | Full permissions for RAM.                                                                                                                                                                |
|                                                            |                          | RAM ReadOnlyAccess                 |        | Read-only permissions for RAM.                                                                                                                                                           |
|                                                            |                          | RAM ResourceShareParticipantAccess |        | Permissions for accepting or reject a resource sharing invitation.                                                                                                                       |
| Organizations<br>(Global service)                          | Global services          | Organizations FullAccess           | Policy | Full permissions for Organizations.                                                                                                                                                      |

| Service | Scope | Policy/Role Name            | Type | Description                              |
|---------|-------|-----------------------------|------|------------------------------------------|
|         |       | OrganizationsReadOnlyAccess |      | Read-only permissions for Organizations. |

## Application

| Service                                                    | Scope                    | Policy/Role Name              | Type   | Description                                                                                                                                                                                                            |
|------------------------------------------------------------|--------------------------|-------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ServiceStage<br>(Project-level service)                    | Region-specific projects | ServiceStage Administrator    | Role   | ServiceStage administrator, who has full permissions for this service.                                                                                                                                                 |
|                                                            |                          | ServiceStage Developer        |        | ServiceStage developer, who has full permissions for this service but does not have the permission for creating infrastructure.                                                                                        |
|                                                            |                          | ServiceStage Operator         |        | ServiceStage operator, who has the read-only permission for this service.                                                                                                                                              |
|                                                            |                          | ServiceStage FullAccess       | Policy | Full permissions for ServiceStage.                                                                                                                                                                                     |
|                                                            |                          | ServiceStage ReadOnlyAccesses |        | Read-only permissions for ServiceStage.                                                                                                                                                                                |
|                                                            |                          | ServiceStage Development      |        | Developer permissions for ServiceStage, including permissions for performing operations on applications, components, and environments, but excluding approval permissions and permissions for creating infrastructure. |
| Cloud Service Engine (CSE)                                 | Region-specific projects | CSE FullAccess                | Policy | Full permissions for CSE.                                                                                                                                                                                              |
|                                                            |                          | CSE ReadOnlyAccesses          |        | Read-only permissions for CSE.                                                                                                                                                                                         |
| Distributed Cache Service (DCS)<br>(Project-level service) | Region-specific projects | DCS FullAccess                | Policy | Full permissions for DCS.                                                                                                                                                                                              |
|                                                            |                          | DCS UserAccess                |        | Common user permissions for DCS operations except creating, modifying, deleting, and scaling instances.                                                                                                                |

| Service                                                                                     | Scope                    | Policy/Role Name   | Type   | Description                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------|--------------------------|--------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                             |                          | DCS ReadOnlyAccess |        | Read-only permissions for DCS.                                                                                                                                                                                                                                                                                                                              |
|                                                                                             |                          | DCS Administrator  | Role   | Full permissions for DCS.<br>This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project.                                                                                                                                                                                                        |
| Distributed Message Service (DMS for Kafka and DMS for RabbitMQ)<br>(Project-level service) | Region-specific projects | DMS UserAccess     | Policy | Common user permissions for DMS (DMS for Kafka and DMS for RabbitMQ), excluding permissions for creating, modifying, deleting, scaling up instances and dumping.                                                                                                                                                                                            |
|                                                                                             |                          | DMS ReadOnlyAccess |        | Read-only permissions for DMS (DMS for Kafka and DMS for RabbitMQ). Users granted these permissions can only view DMS data.                                                                                                                                                                                                                                 |
|                                                                                             |                          | DMS FullAccess     |        | Administrator permissions for DMS (DMS for Kafka and DMS for RabbitMQ). Users granted these permissions can perform all operations on DMS.                                                                                                                                                                                                                  |
| Simple Message Notification (SMN)<br>(Project-level service)                                | Region-specific projects | SMN Administrator  | Role   | Full permissions for SMN.<br>This role must be used together with the <b>Tenant Guest</b> role in the same project.                                                                                                                                                                                                                                         |
|                                                                                             |                          | SMN FullAccess     | Policy | Full permissions for SMN.                                                                                                                                                                                                                                                                                                                                   |
|                                                                                             |                          | SMN ReadOnlyAccess |        | Read-only permissions for SMN.                                                                                                                                                                                                                                                                                                                              |
| API Gateway<br>(Project-level service)                                                      | Region-specific projects | APIG Administrator | Role   | Administrator permissions for API Gateway. Users granted these permissions can use all functions of the <b>shared</b> and <b>dedicated</b> gateways.<br>To use VPC channels, the user must also be assigned the <b>VPC Administrator</b> role.<br>To use custom authentication, the user must also be assigned the <b>FunctionGraph Administrator</b> role. |

| Service                                                            | Scope                    | Policy/Role Name     | Type   | Description                                                                                                                                                                    |
|--------------------------------------------------------------------|--------------------------|----------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                    |                          | APIG FullAccess      | Policy | Full permissions for API Gateway. Users granted these permissions can use all functions of <b>dedicated</b> API gateways.                                                      |
|                                                                    |                          | APIG ReadOnlyAccess  |        | Read-only permissions for API Gateway. Users granted these permissions can only view <b>dedicated</b> API gateways.                                                            |
| Multi-Site High Availability Service (MAS) (Project-level service) | Region-specific projects | MAS FullAccess       | Policy | Full permissions for MAS.                                                                                                                                                      |
|                                                                    |                          | MAS ReadOnlyAccess   |        | Read-only permissions for MAS.                                                                                                                                                 |
|                                                                    |                          | MAS CommonOperations |        | Basic operation permissions for MAS, including the permissions to operate applications, components, and monitors, but excluding the permissions to create or delete instances. |
| Blockchain Service (BCS) (Project-level service)                   | Region-specific projects | BCS Administrator    | Role   | Administrator permissions for BCS.                                                                                                                                             |

## DeC

| Service                                                             | Scope                    | Policy/Role Name   | Type | Description                    |
|---------------------------------------------------------------------|--------------------------|--------------------|------|--------------------------------|
| Dedicated Distributed Storage Service (DSS) (Project-level service) | Region-specific projects | DSS FullAccess     | Role | Full permissions for DSS.      |
|                                                                     |                          | DSS ReadOnlyAccess |      | Read-only permissions for DSS. |



## Database

| Service                                                      | Scope                    | Policy/Role Name   | Type   | Description                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------|--------------------------|--------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Relational Database Service (RDS)<br>(Project-level service) | Region-specific projects | RDS FullAccess     | Policy | Full permissions for RDS.                                                                                                                                                                                                                                                                                                               |
|                                                              |                          | RDS ReadOnlyAccess |        | Read-only permissions for RDS.                                                                                                                                                                                                                                                                                                          |
|                                                              |                          | RDS ManageAccess   |        | Database administrator permissions for all operations except deleting RDS resources.                                                                                                                                                                                                                                                    |
|                                                              |                          | RDS Administrator  | Role   | Full permissions for RDS. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project.                                                                                                                                                                                       |
| Document Database Service (DDS)<br>(Project-level service)   | Region-specific projects | DDS FullAccess     | Policy | Full permissions for DDS.                                                                                                                                                                                                                                                                                                               |
|                                                              |                          | DDS ReadOnlyAccess |        | Read-only permissions for DDS.                                                                                                                                                                                                                                                                                                          |
|                                                              |                          | DDS ManageAccess   |        | Database administrator permissions for all operations except deleting DDS resources.                                                                                                                                                                                                                                                    |
|                                                              |                          | DDS Administrator  | Role   | Full permissions for DDS. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project.<br><br>If a DDS enterprise project is configured, you need to assign the <b>DAS Admin</b> role to users in the same project so that the users can log in to DAS from the DDS console. |

| Service                                                          | Scope                    | Policy/Role Name        | Type   | Description                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------|--------------------------|-------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Replication Service (DRS)<br>(Project-level service)        | Region-specific projects | DRS Administrator       | Role   | Full permissions for DRS. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project.                                                                                                                                                                    |
|                                                                  |                          | DRS FullAccess          | Policy | Full permissions for DRS.                                                                                                                                                                                                                                                                                            |
|                                                                  |                          | DRS ReadOnlyAccess      |        | Read-only permissions for DRS.                                                                                                                                                                                                                                                                                       |
| Data Admin Service (DAS)<br>(Project-level service)              | Region-specific projects | DAS Administrator       | Role   | DAS administrator with full permissions. This role must be used together with the <b>Tenant Guest</b> role in the same project.                                                                                                                                                                                      |
|                                                                  |                          | DAS FullAccess          | Policy | Full permissions for DAS.                                                                                                                                                                                                                                                                                            |
| Distributed Database Middleware (DDM)<br>(Project-level service) | Region-specific projects | DDM FullAccess          | Policy | Full permissions for DDM.                                                                                                                                                                                                                                                                                            |
|                                                                  |                          | DDM CommonOperations    |        | Common permissions for DDM. Users with common permissions cannot perform the following operations: <ul style="list-style-type: none"> <li>• Buying DDM instances</li> <li>• Deleting DDM instances</li> <li>• Scaling up instances</li> <li>• Rolling back instances or clearing data when scale-up fails</li> </ul> |
|                                                                  |                          | DDM ReadOnlyAccess      |        | Read-only permissions for DDM.                                                                                                                                                                                                                                                                                       |
| GeminiDB (Project-level service)                                 | Region-specific projects | GeminiDB FullAccess     | Policy | Full permissions for multi-model NoSQL databases.                                                                                                                                                                                                                                                                    |
|                                                                  |                          | GeminiDB ReadOnlyAccess |        | Read-only permissions for multi-model NoSQL databases.                                                                                                                                                                                                                                                               |

| Service                            | Scope                    | Policy/Role Name       | Type   | Description                        |
|------------------------------------|--------------------------|------------------------|--------|------------------------------------|
| GaussDB<br>(Project-level service) | Region-specific projects | GaussDB FullAccess     | Policy | Full permissions for GaussDB.      |
|                                    |                          | GaussDB ReadOnlyAccess |        | Read-only permissions for GaussDB. |

## Migration

| Service                                               | Scope                    | Policy/Role Name             | Type   | Description                                                                                                                                       |
|-------------------------------------------------------|--------------------------|------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Data Migration (CDM)<br>(Project-level service) | Region-specific projects | CDM Administrator            | Role   | Full permissions for CDM. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project. |
|                                                       |                          | CDM FullAccess               | Policy | Administrator permissions for performing all operations on CDM.                                                                                   |
|                                                       |                          | CDMFullAccessExceptUpdateEIP |        | Permissions for performing all operations except binding and unbinding EIPs on CDM.                                                               |
|                                                       |                          | CDM CommonOperations         |        | Permissions for performing operations on CDM jobs and links.                                                                                      |
|                                                       |                          | CDM ReadOnlyAccess           |        | Read-only permissions for CDM. Users granted these permissions can only view CDM clusters, links, and jobs.                                       |
| Server Migration Service (SMS)<br>(Global service)    | Global services          | SMS FullAccess               | Policy | Full permissions for SMS.                                                                                                                         |
|                                                       |                          | SMS ReadOnlyAccess           |        | Read-only permissions for SMS.                                                                                                                    |

| Service                                                           | Scope                    | Policy/Role Name       | Type   | Description                                                                                                                                                                      |
|-------------------------------------------------------------------|--------------------------|------------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Storage Migration Service (OMS)<br>(Project-level service) | Region-specific projects | OMS Administrator      | Role   | Full permissions for OMS. To use OMS, an IAM user must also be assigned the <b>OBS OperateAccess</b> policy.                                                                     |
| Migration Center (MgC)<br>(Global service)                        | Global services          | MgC FullAccess         | Policy | Administrator permissions for MgC. Users with these permissions can perform all operations on MgC.                                                                               |
|                                                                   |                          | MgC ReadOnlyAccess     |        | Read-only permissions for MgC. Users with these permissions can only view MgC resources.                                                                                         |
|                                                                   |                          | MgC DiscoveryAccess    |        | Permissions for resource discovery with MgC. Users with these permissions can use the resource discovery function of MgC and view MgC resources.                                 |
|                                                                   |                          | MgC AssessAccess       |        | Permissions for application assessment with MgC. Users with these permissions can use the resource discovery and application assessment functions of MgC and view MgC resources. |
|                                                                   |                          | MgC MigrateAccess      |        | Permissions for application migration with MgC. Users with these permissions can use the resource discovery, assessment, and migration functions of MgC and view MgC resources.  |
|                                                                   |                          | MgC AppDiscoveryAccess |        | Permissions for resource discovery with MgC. Users with these permissions can use the resource discovery and collection functions of MgC and view MgC resources.                 |

## Intelligent Edge

| Service                          | Scope           | Policy/Role Name   | Type   | Description                                                                                                                          |
|----------------------------------|-----------------|--------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------|
| CloudLake (IEC) (Global service) | Global services | IEC FullAccess     | Policy | Full permissions for IEC. Users with these permissions can perform any operations on IEC resources.                                  |
|                                  |                 | IEC ReadOnlyAccess |        | Read-only permissions for IEC. Users with these permissions can only view IEC data, for example, viewing the usage of IEC resources. |

## Enterprise Intelligence

| Service                                 | Scope                    | Policy/Role Name           | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|--------------------------|----------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ModelArts (Project-level service)       | Region-specific projects | ModelArts FullAccess       | Policy | Administrator permissions for performing all operations on ModelArts.                                                                                                                                                                                                                                                                                                                      |
|                                         |                          | ModelArts CommonOperations |        | Permissions for performing all operations except managing dedicated resource pools on ModelArts.                                                                                                                                                                                                                                                                                           |
| DataArts Studio (Project-level service) | Region-specific projects | DAYU Administrator         | Role   | <p>Full permissions for DataArts Studio. Users with the <b>DAYU Administrator</b> role have all permissions for workspaces.</p> <p>Only DAYU Administrator has the permission to configure default items of DataArts Factory (including the periodic scheduling, multi-IF policy, hard and soft lock policy, and format of script variables). DAYU User does not have this permission.</p> |

| Service                                            | Scope                    | Policy/Role Name     | Type   | Description                                                                                                                                       |
|----------------------------------------------------|--------------------------|----------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                    |                          | DAYU User            |        | Common DataArts Studio user.<br>Users with the <b>DAYU User</b> role have the permissions of the role assigned to them in a workspace.            |
| MapReduce Service (MRS)<br>(Project-level service) | Region-specific projects | MRS FullAccess       | Policy | Full permissions for MRS.                                                                                                                         |
|                                                    |                          | MRS CommonOperations |        | Common user permissions for MRS operations except creating and deleting resources.                                                                |
|                                                    |                          | MRS ReadOnlyAccess   |        | Read-only permissions for MRS.                                                                                                                    |
|                                                    |                          | MRS Administrator    | Role   | Full permissions for MRS. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project. |
| GaussDB(DWS)                                       | Region-specific projects | DWS FullAccess       | Policy | Full permissions for DWS.                                                                                                                         |
|                                                    |                          | DWS ReadOnlyAccess   |        | Read-only permissions for DWS.                                                                                                                    |
|                                                    |                          | DWS Administrator    | Role   | Full permissions for DWS. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project. |
|                                                    |                          | DWS Database Access  |        | Permissions for accessing DWS. Users granted these permissions can generate temporary tokens for connecting to DWS cluster databases.             |

| Service                                               | Scope                    | Policy/Role Name   | Type   | Description                                                                                                                                                                                                           |
|-------------------------------------------------------|--------------------------|--------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Lake Insight (DLI)<br>(Project-level service)    | Region-specific projects | DLI Service Admin  | Role   | Full permissions for DLI.                                                                                                                                                                                             |
|                                                       |                          | DLI FullAccess     | Policy | Full permissions for DLI. Users granted these permissions can perform all operations on DLI.                                                                                                                          |
|                                                       |                          | DLI ReadOnlyAccess |        | Users granted these permissions can only view the queue list, job list, job details, database list, table list, table creation statements, table fields, and job metadata such as job creation, update, and deletion. |
| Graph Engine Service (GES)<br>(Project-level service) | Region-specific projects | GES Administrator  | Role   | Full permissions for GES. This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project.                                                                     |
|                                                       |                          | GES Manager        |        | Advanced user of GES with permissions for performing any operations on GES resources except creating and deleting graphs. This role must be used together with the <b>Tenant Guest</b> role in the same project.      |
|                                                       |                          | GES Operator       |        | Permissions for viewing and accessing graphs. This role must be used together with the <b>Tenant Guest</b> role in the same project.                                                                                  |
|                                                       |                          | GES FullAccess     | Policy | Administrator permissions for performing all operations (including creation, deletion, access, and upgrade operations) on GES.                                                                                        |

| Service                                                     | Scope                    | Policy/Role Name         | Type | Description                                                                                                                                                 |
|-------------------------------------------------------------|--------------------------|--------------------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                             |                          | GES Development          |      | Operator permissions for all operations except creating and deleting graphs.                                                                                |
|                                                             |                          | GES ReadOnlyAccess       |      | Read-only permissions for viewing resources, such as graphs, metadata, and backup data.                                                                     |
| Cloud Search Service (CSS)<br>(Project-level service)       | Region-specific projects | CSS Administrator        | Role | Full permissions for CSS.<br>This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project.        |
| Data Ingestion Service (DIS)<br>(Project-level service)     | Region-specific projects | DIS Administrator        | Role | Full permissions for DIS.                                                                                                                                   |
|                                                             |                          | DIS Operator             |      | Permissions for managing streams, such as creating and deleting streams, but not for uploading and downloading data.                                        |
|                                                             |                          | DIS User                 |      | Permissions for uploading and downloading data, but not for managing streams.                                                                               |
| CloudTable Service (CloudTable)<br>(Project-level service)  | Region-specific projects | CloudTable Administrator | Role | Full permissions for CloudTable.<br>This role must be used together with the <b>Tenant Guest</b> and <b>Server Administrator</b> roles in the same project. |
| Conversational Bot Service (CBS)<br>(Project-level service) | Region-specific projects | CBS Administrator        | Role | Full permissions for CBS.                                                                                                                                   |
|                                                             |                          | CBS Guest                |      | Read-only permissions for CBS.                                                                                                                              |



| Service                                                                 | Scope                    | Policy/Role Name         | Type   | Description                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------|--------------------------|--------------------------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Huawei HiLens<br>(Project-level service)                                | Region-specific projects | HiLens FullAccess        | Policy | Administrator permissions for Huawei HiLens. Users granted these permissions can operate and use all Huawei HiLens resources.<br><b>If you want to grant permission to participate in OBT, receive alarms, and set skill messages, assign the SMN Administrator role in the same project.</b> |
|                                                                         |                          | HiLens CommonOperations  |        | Operation permissions for Huawei HiLens. Users granted these permissions can perform operations on Huawei HiLens, except deregistering devices and suspending skills.                                                                                                                         |
|                                                                         |                          | HiLens ReadOnlyAccess    |        | Read-only permissions for Huawei HiLens. Users granted these permissions can only view Huawei HiLens data.<br><b>If you want to grant permission to participate in OBT, receive alarms, and set skill messages, assign the SMN Administrator role in the same project.</b>                    |
| Trusted Intelligent Computing Service (TICS)<br>(Project-level service) | Region-specific projects | TICS FullAccess          | Policy | Full permissions for TICS.                                                                                                                                                                                                                                                                    |
|                                                                         |                          | TICS ReadOnlyAccess      |        | Read-only permissions for TICS.                                                                                                                                                                                                                                                               |
|                                                                         |                          | TICS CommonOperations    |        | Permissions for managing alliances, jobs, agents, notifications, and datasets in TICS.                                                                                                                                                                                                        |
| LakeFormation                                                           | Global services          | LakeFormation FullAccess | Policy | Administrator permissions for LakeFormation. Users with these permissions can perform all operations on LakeFormation.                                                                                                                                                                        |

| Service | Scope | Policy/Role Name            | Type | Description                                                                                                                                                                              |
|---------|-------|-----------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |       | LakeFormationReadOnlyAccess |      | Read-only permissions for LakeFormation. Users with these permissions can only view LakeFormation data.                                                                                  |
|         |       | LakeFormationCommonAccess   |      | Basic permissions for LakeFormation, including viewing, authorizing, and canceling the LakeFormation service agreement and basic permissions for dependent services such as OBS and TMS. |

## Enterprise Application

| Service                              | Scope                    | Policy/Role Name         | Type   | Description                                       |
|--------------------------------------|--------------------------|--------------------------|--------|---------------------------------------------------|
| Workspace<br>(Project-level service) | Region-specific projects | WorkspaceFullAccess      | Policy | Full permissions for Workspace.                   |
|                                      |                          | WorkspaceDesktopsManager |        | Desktop administrator permissions for Workspace.  |
|                                      |                          | WorkspaceUserManager     |        | User administrator permissions for Workspace.     |
|                                      |                          | WorkspaceSecurityManager |        | Security administrator permissions for Workspace. |
|                                      |                          | WorkspaceTenantManager   |        | Tenant administrator permissions for Workspace.   |
|                                      |                          | WorkspaceReadOnlyAccess  |        | Read-only permissions for Workspace.              |

| Service                                 | Scope                    | Policy/Role Name      | Type   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|--------------------------|-----------------------|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ROMA Connect<br>(Project-level service) | Region-specific projects | ROMA Administrator    | Role   | <p>Administrator permissions for ROMA Connect. Users with these permissions can perform all operations on ROMA Connect.</p> <p>This role must be used together with the following dependence roles in the same project:</p> <ul style="list-style-type: none"> <li>To use VPC channels, the user must also be assigned the <b>VPC Administrator</b> role.</li> <li>To use FunctionGraph as the backend service of APIs, the user must also be assigned the <b>FunctionGraph Administrator</b> role.</li> <li>To use a rule engine to forward data to DIS, the user must also be assigned the <b>DIS Administrator</b> role.</li> </ul> |
|                                         |                          | ROMA FullAccess       | Policy | All permissions for ROMA Connect. Users granted these permissions can use all ROMA Connect instances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                                         |                          | ROMA CommonOperations |        | Common user permissions for ROMA Connect. This policy does not include permissions for creating, modifying, and deleting instances.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                                         |                          | ROMA ReadOnlyAccess   |        | Read-only permissions for ROMA Connect. Users granted these permissions can only view ROMA Connect data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Service                                                | Scope         | Policy/Role Name           | Type   | Description                         |
|--------------------------------------------------------|---------------|----------------------------|--------|-------------------------------------|
| ROMA Exchange<br>(Global/<br>project-level<br>service) | All resources | ROMAExchange<br>FullAccess | Policy | Full permissions for ROMA Exchange. |
|                                                        |               |                            |        |                                     |
|                                                        |               |                            |        |                                     |

## Cloud Communications

| Service                                      | Scope                       | Policy/Role Name             | Type   | Description                                                                                                                                                                                                |
|----------------------------------------------|-----------------------------|------------------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Voice Call<br>(Project-level<br>service)     | Region-specific<br>projects | RTC Administrator            | Role   | Full permissions for Voice Call, Message & SMS, and Private Number.                                                                                                                                        |
| Message & SMS<br>(Project-level<br>service)  | Region-specific<br>projects | RTC Administrator            | Role   | Full permissions for Voice Call, Message & SMS, and Private Number.                                                                                                                                        |
|                                              |                             | MSGSMS FullAccess            | Policy | Common user permissions for Message & SMS. Users granted these permissions can perform all operations supported by Message & SMS, including creation, deletion, and viewing, and modifying specifications. |
|                                              |                             | MSGSMS ReadOnlyAccess        |        | Read-only permissions for Message & SMS. Users granted these permissions can only view Message & SMS statistics.                                                                                           |
| Private Number<br>(Project-level<br>service) | Region-specific<br>projects | RTC Administrator            | Role   | Full permissions for Voice Call, Message & SMS, and Private Number.                                                                                                                                        |
|                                              |                             | PrivateNumber FullAccess     | Policy | Full permissions for Private Number.                                                                                                                                                                       |
|                                              |                             | PrivateNumber ReadOnlyAccess |        | Read-only permissions for Private Number.                                                                                                                                                                  |

## Video

| Service                                                  | Scope                    | Policy/Role Name        | Type   | Description                                                                                                                                                              |
|----------------------------------------------------------|--------------------------|-------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Media Processing Center (MPC)<br>(Project-level service) | Region-specific projects | MPC Administrator       | Role   | Full permissions for MPC.                                                                                                                                                |
| Video on Demand (VOD)<br>(Project-level service)         | Region-specific projects | VOD Administrator       | Role   | Full permissions for operations on all media files.                                                                                                                      |
|                                                          |                          | VOD Group Administrator |        | Permissions for operations (except global configuration and domain name management) on media files created by users in the current group.                                |
|                                                          |                          | VOD Group Operator      |        | Permissions for operations (except media review, media deletion, global configuration, and domain name management) on media files created by users in the current group. |
|                                                          |                          | VOD Group Guest         |        | Permissions for querying media files created by users in the current group.                                                                                              |
|                                                          |                          | VOD Operator            |        | Permissions for operations (except media review, global configuration, and domain name management) on video files created by users in the current group.                 |
|                                                          |                          | VOD Guest               |        | Read-only permissions for VOD.                                                                                                                                           |
|                                                          |                          | VOD FullAccess          | Policy | Full permissions for VOD.                                                                                                                                                |
|                                                          |                          | VOD ReadOnlyAccess      |        | Read-only permissions for VOD.                                                                                                                                           |

| Service                                        | Scope                    | Policy/Role Name     | Type   | Description                                                                                                                                                                        |
|------------------------------------------------|--------------------------|----------------------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                |                          | VOD CommonOperations |        | Basic operation permissions for VOD, excluding permissions for global configuration, domain name management, permissions management, settings review, and audio and video hosting. |
| Live (Project-level service)                   | Region-specific projects | Live FullAccess      | Policy | Full permissions for Live.                                                                                                                                                         |
|                                                |                          | Live ReadOnlyAccess  |        | Read-only permissions for Live.                                                                                                                                                    |
| Real-Time Communication (RTC) (Global service) | Global services          | RTC FullAccess       | Policy | Full permissions for RTC.                                                                                                                                                          |
|                                                |                          | RTC ReadOnlyAccess   |        | Read-only permissions for RTC.                                                                                                                                                     |

## Development and O&M

| Service                                     | Scope                    | Policy/Role Name                | Type   | Description                                     |
|---------------------------------------------|--------------------------|---------------------------------|--------|-------------------------------------------------|
| CodeArts (Project-level service)            | Region-specific projects | DevCloud Console FullAccess     | Policy | Full permissions for the DevCloud console.      |
|                                             |                          | DevCloud Console ReadOnlyAccess |        | Read-only permissions for the DevCloud console. |
| CodeArts Req (Project-level service)        | Region-specific projects | ProjectMan ConfigOperations     | Policy | Full permissions for ProjectMan.                |
| CodeArts IDE Online (Project-level service) | Region-specific projects | CloudIDE FullAccess             | Policy | Full permissions for CodeArts IDE Online.       |
|                                             |                          | CloudIDE ReadOnlyAccess         |        | Read-only permissions for CodeArts IDE Online.  |

| Service | Scope | Policy/Role Name            | Type | Description                                                                                                                                                      |
|---------|-------|-----------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |       | CloudIDE Development        |      | Development permissions for CodeArts IDE Online, including the permissions for viewing, starting, stopping, and accessing instances.                             |
|         |       | CloudIDE InstanceManagement |      | Instance management permissions for CodeArts IDE Online. Users with these permissions can manage their own instances and access the instances allocated to them. |

## User Support

| Service                                                                                                                                                 | Scope                    | Policy/Role Name                  | Type   | Description                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|-----------------------------------|--------|------------------------------------------------------------------------------------------------------|
| Business Support System (BSS)<br>(Project-level service)<br><b>NOTICE</b><br>These are the projects where permissions for this service can be assigned. | Region-specific projects | BSS Administrator                 | Role   | Full permissions for Billing Center, Resource Center, and My Account.                                |
|                                                                                                                                                         |                          | BSS ReadonlyAccess                | Policy | Read-only permissions for Billing Center, Cost Center, and Message Center.                           |
|                                                                                                                                                         |                          | BSS FinanceAccess                 |        | Financial administrator of BSS in Billing Center, who has full permissions for financial operations. |
|                                                                                                                                                         |                          | Enterprise Project BSS FullAccess |        | All operations permissions supported by Enterprise Project.                                          |
| Enterprise Project Management Service (EPS)<br>(Global service)                                                                                         | Global services          | EPS FullAccess                    | Policy | Full permissions for EPS.                                                                            |
|                                                                                                                                                         |                          | EPS ReadonlyAccess                |        | Read-only permissions for EPS.                                                                       |

| Service                                                 | Scope           | Policy/Role Name      | Type   | Description                                                                        |
|---------------------------------------------------------|-----------------|-----------------------|--------|------------------------------------------------------------------------------------|
| Service Ticket<br>(Global service)                      | Global services | Ticket Administrator  | Role   | Full permissions for Service Ticket.                                               |
|                                                         |                 | Ticket Group Operator |        | Permissions for processing service tickets of other users in the same group.       |
| Professional Services<br>(Global/project-level service) | All resources   | PSDMFullAccess        | Policy | Full permissions for the Professional Service Delivery Management (PSDM) platform. |
|                                                         |                 | PSDMReadOnlyAccess    |        | Read-only permissions for the PSDM platform.                                       |
| ICP License Service<br>(Global service)                 | Global services | Beian Administrator   | Role   | ICP License Service administrator with full permissions.                           |

## Other

| Service                            | Scope           | Policy/Role Name                 | Type   | Description                                                                                                                                                                    |
|------------------------------------|-----------------|----------------------------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message Center<br>(Global service) | Global services | MessageCenterFullAccess          | Policy | Full permissions for Message Center.                                                                                                                                           |
|                                    |                 | MessageCenterReadOnlyAccess      |        | Read-only permissions for Message Center.                                                                                                                                      |
|                                    |                 | MessageCenterRecipientManagement |        | Message receiving management permissions for Message Center, including permissions for configuring SMS messages, emails, and voice messages, viewing and modifying recipients. |



# 2 System-defined Identity Policies

New IAM users do not have any permissions assigned by default. You need to attach identity policies to the users or add them to one or more groups and attach identity policies to these groups on the new IAM console. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

IAM provides system-defined identity policies to define common actions supported by cloud services. System-defined identity policies cannot be modified. They can be directly used to assign permissions to users.

If there are no system-defined identity policies for a specific service, it indicates that IAM does not support this service. The administrator can [submit a service ticket](#) and request to register permissions for that service in IAM.

If system-defined identity policies cannot meet your requirements, you can create custom identity policies for more refined access control. For the permissions, resources, and condition keys supported by each service, see [3 Identity Policy-based Authorization](#).

## Global

| Service         | Identity Policy            | Description                                                                                                                                                       |
|-----------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Global services | ReadOnlyPolicy             | Read-only permissions for all services.                                                                                                                           |
| Global services | AdministratorAccess-Policy | Full permissions for all services.<br><b>NOTE</b><br>All services refer to the <a href="#">cloud services that support identity policies and trust agencies</a> . |

## Compute

| Service                        | Identity Policy               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Elastic Cloud Server (ECS)     | ECSFullPolicy                 | Full permissions for ECS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                | ECSCCommonOperationsPolicy    | Common user permissions for ECS. Users granted these permissions can query, start, stop, and restart ECSs, manage automatic recovery of an ECS, reset the password for logging in to an ECS with a few clicks, configure a private IP address for a NIC of an ECS, obtain the address for remotely logging in to an ECS using VNC, obtain EVS disk information, configure security group rules, manage ECS groups, use float IP addresses and key pairs, manage the password to log in to a Windows ECS, obtain the address for logging in to the console using VNC, create images, configure ECS metadata, add tags to an ECS, use ECS disks, query the disks attached to an ECS, query NICs of an ECS, and create, query, and delete IMS images. |
|                                | ECSReadOnlyPolicy             | Read-only permissions for ECS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                | ECSPartnerOperationsPolicy    | Partner permissions for ECS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Bare Metal Server (BMS)        | BMSFullPolicy                 | Full permissions for BMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                | BMSReadOnlyPolicy             | Read-only permissions for BMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                | BMSCommonOperationsPolicy     | Common user permissions for BMS. Users with these permissions can start, stop, restart, and query BMSs, and attach a data disk to and detach a data disk from a BMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Auto Scaling                   | ASFullPolicy                  | Full permissions for Auto Scaling.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                | ASReadOnlyPolicy              | Read-only permissions for Auto Scaling.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                                | ASServiceLinkedAgencyPolicy   | Permissions of service-linked agencies for Auto Scaling.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Image Management Service (IMS) | IMSFullAccessPolicy           | Full permissions for IMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                                | IMSReadOnlyPolicy             | Read-only permissions for IMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| FunctionGraph                  | FunctionGraphFullAccessPolicy | Full permissions for FunctionGraph.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                                | FunctionGraphReadOnlyPolicy   | Read-only permissions for FunctionGraph.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Service | Identity Policy                        | Description                                                                      |
|---------|----------------------------------------|----------------------------------------------------------------------------------|
|         | FunctionGraphCommonOperationsPolicy    | Invoker permissions for querying functions and triggers, and invoking functions. |
|         | FunctionGraphServiceLinkedAgencyPolicy | Agency permissions for FunctionGraph to access VPC and mount disks.              |

## Storage

| Service                         | Identity Policy                     | Description                                                                                                                                                                                                                                          |
|---------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Storage Service (OBS)    | OBSBucketsViewerPolicy              | Permissions for viewing the bucket list, obtaining bucket metadata, and querying the bucket location in OBS.                                                                                                                                         |
|                                 | OBSFullAccessPolicy                 | Administrator permissions for OBS.                                                                                                                                                                                                                   |
|                                 | OBSConsoleFullAccessPolicy          | Permissions for all operations on the OBS console.                                                                                                                                                                                                   |
|                                 | OBSBasicOperationsPolicy            | Permissions for basic operations on OBS, such as viewing the bucket list, obtaining bucket metadata, listing objects in a bucket, querying the bucket location, uploading objects, obtaining objects, deleting objects, and obtaining an object ACL. |
|                                 | OBSReadOnlyPolicy                   | Read-only permissions for viewing the bucket list, obtaining bucket metadata, listing objects in a bucket, and querying the bucket location in OBS.                                                                                                  |
| Elastic Volume Service (EVS)    | EVFullAccessPolicy                  | Administrator permissions for using all disks and snapshots on EVS.                                                                                                                                                                                  |
|                                 | EVReadOnlyPolicy                    | Read-only permissions for EVS.                                                                                                                                                                                                                       |
| Cloud Backup and Recovery (CBR) | CBRFullAccessPolicy                 | Administrator permissions for using all vaults, backups, and policies on CBR.                                                                                                                                                                        |
|                                 | CBRReadOnlyPolicy                   | Read-only permissions for CBR.                                                                                                                                                                                                                       |
|                                 | CBRBackupsAndVaultsFullAccessPolicy | Common user permissions for CBR, excluding the permissions for creating, updating, and deleting a policy.                                                                                                                                            |
|                                 | CBRServiceLinkedAgencyPolicy        | Permissions of service-linked agencies for CBR across accounts.                                                                                                                                                                                      |

| Service                     | Identity Policy           | Description                                                                                                    |
|-----------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------|
| Scalable File Service (SFS) | SFSTurboFullAccess-Policy | Administrator permissions for SFS. Users granted these permissions can perform all operations on file systems. |
|                             | SFSTurboReadOnly-Policy   | Read-only permissions for SFS.                                                                                 |

## Networking

| Service                       | Identity Policy            | Description                                                                                                                       |
|-------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Virtual Private Cloud (VPC)   | VPCFullAccessPolicy        | Full permissions for VPC.                                                                                                         |
|                               | VPCReadOnlyPolicy          | Read-only permissions for VPC.                                                                                                    |
|                               | VPCConsoleFullAccessPolicy | Permissions for all operations on the VPC console.                                                                                |
|                               | VPCConsoleReadOnlyPolicy   | Read-only permissions for VPC console.                                                                                            |
| Elastic Load Balance (ELB)    | ELBFullAccessPolicy        | Full permissions for ELB.                                                                                                         |
|                               | ELBReadOnlyAccessPolicy    | Read-only permissions for ELB.                                                                                                    |
| NAT Gateway                   | NATFullAccessPolicy        | Full permissions for NAT Gateway.                                                                                                 |
|                               | NATReadOnlyPolicy          | Read-only permissions for NAT Gateway.                                                                                            |
| Direct Connect                | DCAASFullAccessPolicy      | Full permissions for Direct Connect.                                                                                              |
|                               | DCAASReadOnlyPolicy        | Read-only permissions for Direct Connect.                                                                                         |
| Virtual Private Network (VPN) | VPNFullAccessPolicy        | Full permissions for VPN.                                                                                                         |
|                               | VPNReadOnlyPolicy          | Read-only permissions for VPN.                                                                                                    |
| Domain Name Service (DNS)     | DNSFullAccessPolicy        | Administrator permissions for performing all operations (including creating, deleting, querying, and modifying resources) on DNS. |
|                               | DNSReadOnlyAccessPolicy    | Read-only permissions for DNS. Users granted these permissions can only view DNS resources.                                       |
| VPC Endpoint (VPCEP)          | VPCEPFullAccessPolicy      | Full permissions for VPCEP.                                                                                                       |

| Service            | Identity Policy         | Description                                   |
|--------------------|-------------------------|-----------------------------------------------|
|                    | VPCEPReadOnlyPolicy     | Read-only permissions for VPCEP.              |
| Cloud Connect      | CCFullAccessPolicy      | Full permissions for Cloud Connect.           |
|                    | CCReadOnlyPolicy        | Read-only permissions for Cloud Connect.      |
| Enterprise Router  | ERFullAccessPolicy      | Full permissions for Enterprise Router.       |
|                    | ERReadOnlyPolicy        | Read-only permissions for Enterprise Router.  |
| Elastic IP (EIP)   | EIPReadOnlyAccessPolicy | Read-only permissions for EIP.                |
|                    | EIPFullAccessPolicy     | Full permissions for EIP.                     |
| Global Accelerator | GAFullAccessPolicy      | Full permissions for Global Accelerator.      |
|                    | GAReReadOnlyPolicy      | Read-only permissions for Global Accelerator. |

## Containers

| Service                                 | Identity Policy         | Description                    |
|-----------------------------------------|-------------------------|--------------------------------|
| Cloud Container Engine (CCE)            | CCEFullPolicy           | Full permissions for CCE.      |
|                                         | CCEReReadOnlyPolicy     | Read-only permissions for CCE. |
| Cloud Container Instance (CCI)          | CCIFullAccessPolicy     | Full permissions for CCI.      |
|                                         | CCIReReadOnlyPolicy     | Read-only permissions for CCI. |
| Software Repository for Container (SWR) | SWRReadOnlyAccessPolicy | Read-only permissions for SWR. |
|                                         | SWROperateAccessPolicy  | Operation permissions for SWR. |
|                                         | SWRFullAccessPolicy     | Full permissions for SWR.      |

## Content Delivery & Edge Computing

| Service                        | Identity Policy                                   | Description                                                                                                    |
|--------------------------------|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Content Delivery Network (CDN) | CDNLogsReadOnlyPolicy                             | Read-only permissions for the CDN log service.                                                                 |
|                                | CDNSecurityProtectionConfiguration-ReadOnlyPolicy | Read-only permissions for the CDN security service.                                                            |
|                                | CDNRefreshAndPreheatPolicy                        | Permissions to configure CDN cache refreshing and preheating.                                                  |
|                                | CDNAdministratorPolicy                            | Full permissions for CDN.                                                                                      |
|                                | CDNSecurityProtectionConfigurationPolicy          | Permissions for adding, modifying, and deleting a CDN security policy, and binding or unbinding a domain name. |
|                                | CDNReadOnlyPolicy                                 | Read-only permissions for all CDN services.                                                                    |
|                                | CDNFullPolicy                                     | Full permissions for CDN.                                                                                      |
|                                | CDNStatisticsReadOnlyPolicy                       | Read-only permissions for the CDN statistics service.                                                          |
|                                | CDNSecurityProtectionStatisticsReadOnlyPolicy     | Read-only permissions for CDN security statistics.                                                             |
|                                | CDNDomainConfigurationPolicy                      | Permissions for configuring CDN acceleration domain names.                                                     |
|                                | CDNDomainReadOnlyPolicy                           | Read-only permissions for CDN acceleration domain names.                                                       |
|                                | CDNChargeConfigurationPolicy                      | Permission for enabling CDN billing and modifying and querying the billing option.                             |
|                                | CDNStatisticsFullPolicy                           | Full permissions for the CDN statistics service.                                                               |
| CloudPond                      | IESFullAccessPolicy                               | Full permissions for CloudPond.                                                                                |
|                                | IESReadOnlyPolicy                                 | Read-only permissions for CloudPond.                                                                           |

## Security & Compliance

| Service                                | Identity Policy               | Description                                                                                            |
|----------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------|
| Advanced Anti-DDoS (AAD)               | AADFullAccessPolicy           | Full permissions for AAD.                                                                              |
|                                        | AADReadOnlyAccessPolicy       | AAD read-only permissions. Users with these permissions can only view AAD information.                 |
| Cloud Native Anti-DDoS Advanced (CNAD) | CNADFullAccessPolicy          | Full permissions for CNAD.                                                                             |
|                                        | CNADReadOnlyPolicy            | Read-only permissions for CNAD. Users granted these permissions can only view CNAD resources.          |
| CNAD Basic (Anti-DDoS)                 | Anti-DDoSFullAccessPolicy     | Full permissions for Anti-DDoS.                                                                        |
|                                        | Anti-DDoSReadOnlyPolicy       | Read-only permissions for Anti-DDoS. Users with these permissions can only view Anti-DDoS information. |
| Host Security Service (HSS)            | HSSServiceLinkedAgencyPolicy  | Permissions of service-linked agencies for HSS across accounts.                                        |
|                                        | HSSFullAccessPolicy           | Full permissions for HSS.                                                                              |
|                                        | HSSReadOnlyAccessPolicy       | Read-only permissions for HSS.                                                                         |
|                                        | HSSAdministratorPolicy        | HSS administrator with full permissions.                                                               |
| Database Security Service (DBSS)       | DBSSReadOnlyPolicy            | Read-only permissions for DBSS.                                                                        |
|                                        | DBSSFullAccessPolicy          | Full permissions for DBSS.                                                                             |
|                                        | DBSSServiceLinkedAgencyPolicy | Permissions of service-linked agencies for DBSS.                                                       |
| Data Encryption Workshop (DEW)         | KMSReadOnlyPolicy             | Read-only permissions for KMS.                                                                         |
|                                        | KMSFullAccessPolicy           | Full permissions for KMS.                                                                              |
|                                        | CSMSFullAccessPolicy          | Full permissions for Cloud Secret Management Service (CSMS).                                           |
|                                        | CSMSReadOnlyPolicy            | Read-only permissions for CSMS.                                                                        |
|                                        | CSMSServiceLinkedAgencyPolicy | Permissions of service-linked agencies for CSMS across accounts.                                       |

| Service                                                                                  | Identity Policy                  | Description                                                                                      |
|------------------------------------------------------------------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------|
|                                                                                          | DHSMFullAccessPolicy             | Administrator permissions for DHSM.                                                              |
|                                                                                          | DHSMReadOnlyPolicy               | Read-only permissions for DHSM.                                                                  |
|                                                                                          | KPSFullAccessPolicy              | Full permissions for KPS.                                                                        |
|                                                                                          | KPSReadOnlyPolicy                | Read-only permissions for KPS.                                                                   |
| Web Application Firewall (WAF)                                                           | WAFReadOnlyAccessPolicy          | Read-only permissions for WAF.                                                                   |
|                                                                                          | WAFFullAccessPolicy              | Administrator permissions for WAF.                                                               |
|                                                                                          | WAFServiceLinkedAgencyPolicy     | Permissions of service-linked agencies for WAF across accounts.                                  |
| Cloud Firewall (CFW)                                                                     | CFWFullAccessPolicy              | Full permissions for CFW.                                                                        |
|                                                                                          | CFWReadOnlyPolicy                | Read-only permissions for CFW.                                                                   |
|                                                                                          | CFWServiceLinkedAgencyPolicy     | Permissions of service-linked agencies for CFW across accounts.                                  |
| SSL Certificate Manager (SCM)<br>(Global service)<br>(SCM has been integrated into CCM.) | SCMReadOnlyPolicy                | Read-only permissions for SCM.                                                                   |
|                                                                                          | SCMFullPolicy                    | Administrator permissions for SCM.                                                               |
| Cloud Bastion Host (CBH)                                                                 | CBHFullAccessPolicy              | Full permissions for CBH.                                                                        |
|                                                                                          | CBHReadOnlyPolicy                | Read-only permissions for CBH.                                                                   |
|                                                                                          | CBHServiceLinkedAgencyPolicy     | Agency permissions required for CBH to access KMS and credential management services of tenants. |
| Data Security Center (DSC)                                                               | DSCDashboardReadOnlyAccessPolicy | Read-only permissions for the overview page of DSC.                                              |
|                                                                                          | DSCFullAccessPolicy              | Full permissions for DSC.                                                                        |
|                                                                                          | DSCReadOnlyAccessPolicy          | Read-only permissions for DSC.                                                                   |
|                                                                                          | DSCServiceAgencyPolicy           | Agency permissions for DSC.                                                                      |



| Service                           | Identity Policy                 | Description                                                     |
|-----------------------------------|---------------------------------|-----------------------------------------------------------------|
|                                   | DSCServiceLinkedAgencyPolicy    | Permissions of service-linked agencies for DSC across accounts. |
| Cloud Certificate & Manager (CCM) | PCAFullAccessPolicy             | Full permissions for PCA.                                       |
|                                   | PCAReadOnlyPolicy               | Read-only permissions for PCA.                                  |
|                                   | PCAServiceLinkedAgencyPolicy    | Permissions of service-linked agencies for PCA across accounts. |
| SecMaster                         | SecMasterFullAccess             | Administrator permissions for SecMaster.                        |
|                                   | SecMasterReadOnly               | Read-only permissions for SecMaster.                            |
|                                   | ServiceLinkedAgencyForSecMaster | SecMaster agency policy for connecting with other services.     |

## Management & Governance

| Service                                 | Identity Policy                         | Description                                                     |
|-----------------------------------------|-----------------------------------------|-----------------------------------------------------------------|
| Identity and Access Management (IAM)    | IAMFullAccessPolicy                     | Full permissions for IAM.                                       |
|                                         | IAMReadOnlyPolicy                       | Read-only permissions for IAM.                                  |
|                                         | AccessAnalyzerServiceLinkedAgencyPolicy | Permissions of service-linked agencies for Access Analyzer.     |
| Cloud Eye                               | CESReadOnlyPolicy                       | Read-only permissions for Cloud Eye.                            |
|                                         | CESFullAccessPolicy                     | Full permissions for Cloud Eye.                                 |
|                                         | CESAgentServiceLinkedAgencyPolicy       | Permissions of service-linked agencies for the Cloud Eye Agent. |
| Application Operations Management (AOM) | AOMFullAccessPolicy                     | Full permissions for AOM.                                       |
|                                         | AOMReadOnlyPolicy                       | Read-only permissions for AOM.                                  |
|                                         | AOMServiceLinkedAgencyPolicy            | Permissions of service-linked agencies for AOM across accounts. |
| Cloud Trace Service (CTS)               | CTSFullAccessPolicy                     | Full permissions for CTS.                                       |
|                                         | CTSReadOnlyPolicy                       | Read-only permissions for CTS.                                  |
|                                         | CTSServiceLinkedAgencyPolicy            | Permissions of service-linked agencies for CTS across accounts. |
| Log Tank Service (LTS)                  | LTSFullAccessPolicy                     | Full permissions for LTS.                                       |

| Service                       | Identity Policy                         | Description                                                                                                                     |
|-------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                               | LTSReadOnlyAccessPolicy                 | Read-only permissions for LTS.                                                                                                  |
|                               | LTSServiceLinkedAgencyPolicy            | Organization management permissions for LTS across accounts.                                                                    |
| Tag Management Service (TMS)  | TMSReadOnlyPolicy                       | Read-only permissions for TMS.                                                                                                  |
|                               | TMSFullAccessPolicy                     | Full permissions for TMS.                                                                                                       |
| Config                        | ConfigReadOnlyPolicy                    | Read-only permissions for Config.                                                                                               |
|                               | ConfigFullAccessPolicy                  | Full permissions for Config.                                                                                                    |
|                               | ConfigConsoleFullAccessPolicy           | Permissions for all operations on the Config console.                                                                           |
|                               | RMSRemediationServiceLinkedAgencyPolicy | Permissions of service-linked agencies for Config remediation.                                                                  |
|                               | RMSServiceLinkedAgencyPolicy            | Permissions of service-linked agencies for Config across accounts.                                                              |
|                               | RMSConformsServiceLinkedAgencyPolicy    | Service agencies for conformance package configuration management.                                                              |
| Resource Access Manager (RAM) | RAMFullAccessPolicy                     | Full permissions for RAM.                                                                                                       |
|                               | RAMReadOnlyPolicy                       | Read-only permissions for RAM.                                                                                                  |
|                               | RAMResourceShareParticipantAccessPolicy | Permissions for accepting or reject the invitation to a resource share.                                                         |
| IAM Identity Center           | IdentityCenterFullAccessPolicy          | Administrator permissions for IAM Identity Center. Users with this permission can manage and use IAM Identity Center resources. |
|                               | IdentityCenterReadOnlyPolicy            | Read-only permissions for IAM Identity Center. Users with this permission can only view data on IAM Identity Center.            |
|                               | IdentityCenterServiceLinkedAgencyPolicy | Permissions of service-linked agencies for IAM Identity Center.                                                                 |
| Organizations                 | OrganizationsReadOnlyAccessPolicy       | Read-only permissions for Organizations.                                                                                        |

| Service                          | Identity Policy                        | Description                                                    |
|----------------------------------|----------------------------------------|----------------------------------------------------------------|
|                                  | OrganizationsFullAccessPolicy          | Full permissions for Organizations.                            |
|                                  | OrganizationsServiceLinkedAgencyPolicy | Permissions for creating and deleting service-linked agencies. |
| Resource Formation Service (RFS) | RFFullAccessPolicy                     | Full permissions for RFS.                                      |
|                                  | RFReadOnlyPolicy                       | Read-only permissions for RFS.                                 |
|                                  | RFDeployPolicy                         | Deployment permissions for RFS.                                |
|                                  | RFStackSetFullAccessPolicy             | Full permissions for the stack set.                            |
|                                  | RFStackSetReadOnlyPolicy               | Read-only permissions for the stack set.                       |
| Resource Governance Center (RGC) | RGCServiceLinkedAgencyPolicy           | Permissions for deleting service-linked agencies.              |

## Application

| Service                         | Identity Policy              | Description                                                                                                                                                                                                            |
|---------------------------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ServiceStage                    | ServiceStageFullAccessPolicy | Full permissions for ServiceStage.                                                                                                                                                                                     |
|                                 | ServiceStageReadOnlyPolicy   | Read-only permissions for ServiceStage.                                                                                                                                                                                |
|                                 | ServiceStageDeveloperPolicy  | Developer permissions for ServiceStage, including permissions for performing operations on applications, components, and environments, but excluding approval permissions and permissions for creating infrastructure. |
| Cloud Service Engine (CSE)      | CSEFullAccessPolicy          | Full permissions for CSE.                                                                                                                                                                                              |
|                                 | CSEReadOnlyPolicy            | Permissions for viewing CSE resources.                                                                                                                                                                                 |
|                                 | CSEServiceLinkedAgencyPolicy | Agency permissions required for creating and maintaining CSE instances.                                                                                                                                                |
| Distributed Cache Service (DCS) | DCSFullAccessPolicy          | Full permissions for DCS.                                                                                                                                                                                              |
|                                 | DCSUserAccessPolicy          | Common user permissions for DCS operations except creating, modifying, deleting, and scaling instances.                                                                                                                |

| Service                                                          | Identity Policy              | Description                                                                                                       |
|------------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------|
|                                                                  | DCSReadOnlyAccessPolicy      | Read-only permissions for DCS.                                                                                    |
|                                                                  | DCSServiceLinkedAgencyPolicy | Agency permissions required by DCS for migrating faulty instances.                                                |
| Distributed Message Service (DMS for Kafka and DMS for RabbitMQ) | DMSFullAccessPolicy          | Full permissions for DMS.                                                                                         |
|                                                                  | DMSConsoleFullAccessPolicy   | Full permissions for operations on the DMS console.                                                               |
|                                                                  | DMSUserAccessPolicy          | Common user permissions for DMS, excluding permissions for creating, deleting, scaling up instances, and dumping. |
|                                                                  | DMSReadOnlyAccessPolicy      | Read-only permissions for DMS.                                                                                    |
|                                                                  | DMSServiceLinkedAgencyPolicy | Permissions of service-linked agencies for DMS.                                                                   |
| Simple Message Notification (SMN)                                | SMNFullAccessPolicy          | Full permissions for SMN.                                                                                         |
|                                                                  | SMNReadOnlyPolicy            | Read-only permissions for SMN.                                                                                    |
| API Gateway                                                      | APIGFullAccessPolicy         | Full permissions for APIG.                                                                                        |
|                                                                  | APIGReadOnlyAccessPolicy     | Read-only permissions for APIG.                                                                                   |

## Database

| Service                           | Identity Policy              | Description                                                                                 |
|-----------------------------------|------------------------------|---------------------------------------------------------------------------------------------|
| Relational Database Service (RDS) | RDSFullAccessPolicy          | Full permissions for RDS.                                                                   |
|                                   | RDSReadOnlyPolicy            | Read-only permissions for RDS.                                                              |
|                                   | RDSServiceLinkedAgencyPolicy | Permissions of service-linked agencies for RDS across accounts.                             |
| Document Database Service (DDS)   | DDSFullAccessPolicy          | Full permissions for DDS.                                                                   |
|                                   | DDSReadOnlyPolicy            | Read-only permissions for DDS.                                                              |
|                                   | DDSServiceLinkedAgencyPolicy | Permissions of service-linked agencies for DDS across accounts.                             |
| Data Replication Service (DRS)    | DRSFullAccessPolicy          | Administrator permissions for DRS. Users granted these permissions can operate and use DRS. |

| Service            | Identity Policy                           | Description                                                                    |
|--------------------|-------------------------------------------|--------------------------------------------------------------------------------|
|                    | DRSFullWithOutDeleteAccessPolicy          | Full permissions for DRS, except for those for stopping and deleting tasks.    |
|                    | DRSReadOnlyAccessPolicy                   | Read-only permissions for DRS.                                                 |
|                    | DRSServiceLinkedAgencyPolicy              | Permissions of service-linked agencies for DRS across accounts.                |
| GeminiDB           | GaussDBforNoSQL-FullAccessPolicy          | Full permissions for GeminiDB.                                                 |
|                    | GaussDBforNoSQL-ReadOnlyPolicy            | Read-only permissions for GeminiDB.                                            |
|                    | GaussDBforNoSQL-ServiceLinkedAgencyPolicy | Permissions of service-linked agencies for GeminiDB across accounts.           |
| GaussDB            | GaussDBFullAccessPolicy                   | Full permissions for GaussDB.                                                  |
|                    | GaussDBReadOnlyPolicy                     | Read-only permissions for GaussDB.                                             |
|                    | GaussDBServiceLinkedAgencyPolicy          | Permissions of service-linked agencies for GaussDB across accounts.            |
| GaussDB(for MySQL) | GaussDBforMySQL-ReadOnlyPolicy            | Read-only permissions for GaussDB(for MySQL).                                  |
|                    | GaussDBforMySQL-FullAccessPolicy          | Full permissions for GaussDB(for MySQL).                                       |
|                    | GaussDBforMySQL-ServiceLinkedAgencyPolicy | Permissions of service-linked agencies for GaussDB(for MySQL) across accounts. |

## Migration

| Service                                | Identity Policy     | Description                                                                                                     |
|----------------------------------------|---------------------|-----------------------------------------------------------------------------------------------------------------|
| Server Migration Service (SMS)         | SMSFullAccessPolicy | Full permissions for SMS.                                                                                       |
|                                        | SMSReadOnlyPolicy   | Read-only permissions for SMS.                                                                                  |
| Object Storage Migration Service (OMS) | OMSFullAccessPolicy | Administrator permissions for OMS. Users granted these permissions can create, operate, and view OMS resources. |
|                                        | OMSReadOnlyPolicy   | Full permissions for OMS.                                                                                       |

| Service                | Identity Policy              | Description                                                 |
|------------------------|------------------------------|-------------------------------------------------------------|
| Migration Center (MgC) | MGCFullAccessPolicy          | Full permissions for MgC.                                   |
|                        | MGCReadOnlyPolicy            | Read-only permissions for MgC.                              |
|                        | MGCCollectionAccessPolicy    | Permissions for resource discovery and collection with MgC. |
|                        | MGCAssessmentAccessPolicy    | Permissions for resource assessment with MgC.               |
|                        | MGCManagementAccessPolicy    | Permissions for managing migration settings on MgC.         |
|                        | MGCWorkflowAccessPolicy      | Permissions for using MgC migration workflows.              |
|                        | MGCMigrationPlanAccessPolicy | Permissions for designing migration plans with MgC.         |
|                        | MGCBigdataAccessPolicy       | Permissions for migrating and verifying big data with MgC.  |

## AI

| Service                 | Identity Policy                 | Description                                                                                                   |
|-------------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------|
| ModelArts               | ModelArtsFullAccessPolicy       | Full permissions for ModelArts.                                                                               |
|                         | ModelArtsCommonOperationsPolicy | Common user permissions for ModelArts (excluding creating, updating, and deleting a dedicated resource pool). |
|                         | ModelArtsDependencyAccessPolicy | Permissions for common dependent services of ModelArts.                                                       |
|                         | OptVerseFullAccessPolicy        | Full permissions for OptVerse.                                                                                |
|                         | OptVerseReadOnlyPolicy          | Read-only permissions for OptVerse.                                                                           |
|                         | OptVerseTaskFullAccessPolicy    | Full permissions for OptVerse task management.                                                                |
| MapReduce Service (MRS) | MRSFullAccessPolicy             | Administrator permissions for MRS. Users granted these permissions can operate and use MRS clusters.          |
|                         | MRSReadOnlyAccessPolicy         | Read-only permissions for MRS.                                                                                |
| DWS                     | DWSFullAccessPolicy             | Full permissions for DWS.                                                                                     |

| Service                    | Identity Policy              | Description                                    |
|----------------------------|------------------------------|------------------------------------------------|
|                            | DWSReadOnlyPolicy            | Read-only permissions for DWS.                 |
|                            | DWSAccessVPCPolicy           | Agency permissions for DWS to access VPC.      |
|                            | DWSAccessOBSPolicy           | Agency permissions for DWS to access OBS.      |
|                            | DWSAccessLTSPolicy           | Agency permissions for DWS to access LTS.      |
|                            | DWSAccessKMSPolicy           | Agency permissions for DWS to access KMS.      |
|                            | DWSAccessDWSPolicy           | Agency permissions for DWS to access DWS.      |
| Data Lake Insight (DLI)    | DLIFullAccessPolicy          | Full permissions for DLI.                      |
|                            | DLIReadOnlyPolicy            | Read-only permissions for DLI.                 |
| Cloud Search Service (CSS) | CSSFFullAccessPolicy         | Full permissions for CSS.                      |
|                            | CSSReadOnlyPolicy            | Read-only permissions for CSS.                 |
|                            | CSSAccessVPCPolicy           | Agency permissions for CSS to access VPC.      |
|                            | CSSAccessOBSPolicy           | Agency permissions for CSS to access OBS.      |
|                            | CSSAccessELBPolicy           | Agency permissions for CSS to access ELB.      |
|                            | CSSAccessCSSLog-streamPolicy | Agency permissions for CSS to access CSS logs. |

## Big Data

| Service                 | Identity Policy              | Description                                                                                                                                                       |
|-------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Lake Insight (DLI) | DLIFullAccessPolicy          | Full permissions for DLI.                                                                                                                                         |
|                         | DLIReadOnlyPolicy            | Read-only permissions for DLI.                                                                                                                                    |
| DataArts Studio         | DataArtsStudioReadOnlyPolicy | Full permissions for managing DataArts Studio instances and workspaces, except service operation permissions in workspaces and permissions of dependent services. |

| Service | Identity Policy                | Description                                                                                                                                                                         |
|---------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | DataArtsStudioFullAccessPolicy | Permissions for performing common operations on DataArts Studio instances and workspaces, except service operation permissions in workspaces and permissions of dependent services. |
|         | DataArtsStudioReadOnlyPolicy   | Permissions for viewing DataArts Studio instances and workspaces, except service operation permissions in workspaces and permissions of dependent services.                         |

## Video

| Service                       | Identity Policy            | Description                           |
|-------------------------------|----------------------------|---------------------------------------|
| Media Processing Center (MPC) | MPCFullAccessPolicy        | Full permissions for MPC.             |
|                               | MPCReadOnlyPolicy          | Read-only permissions for MPC.        |
| Live                          | LiveFullAccessPolicy       | Full permissions for Live.            |
|                               | LiveReadOnlyPolicy         | Read-only permissions for Live.       |
| MetaStudio                    | MetaStudioFullAccessPolicy | Full permissions for MetaStudio.      |
|                               | MetaStudioReadOnlyPolicy   | Read-only permissions for MetaStudio. |

## Internet of Things

| Service                   | Identity Policy       | Description                      |
|---------------------------|-----------------------|----------------------------------|
| IoT Device Access (IoTDA) | IoTDAFullAccessPolicy | Full permissions for IoTDA.      |
|                           | IoTDAReadOnlyPolicy   | Read-only permissions for IoTDA. |

## Developer Services

| Service  | Identity Policy          | Description                                |
|----------|--------------------------|--------------------------------------------|
| CodeArts | CODEARTSFullAccessPolicy | Full permissions for the CodeArts console. |



| Service           | Identity Policy                             | Description                                       |
|-------------------|---------------------------------------------|---------------------------------------------------|
|                   | CODEARTSReadOnlyPolicy                      | Read-only permissions for the CodeArts console.   |
| CodeArts Pipeline | CODEARTSPIPELINE-FullAccessPolicy           | Full permissions for CodeArts Pipeline.           |
|                   | CODEARTSPIPELINE-ReadOnlyPolicy             | Read-only permissions for CodeArts Pipeline.      |
|                   | CODEARTSPIPELINE-TemplateFullAccess-Policy  | Full permissions for pipeline templates.          |
|                   | CODEARTSPIPELINE-RuleFullAccessPolicy       | Full permissions for pipeline rules.              |
|                   | CODEARTSPIPELINE-StrategyFullAccess-Policy  | Full permissions for pipeline policies.           |
|                   | CODEARTSPIPELINE-ExtensionFullAccess-Policy | Full permissions for pipeline extension plug-ins. |

## Customer Services

| Service                       | Identity Policy          | Description                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Business Support System (BSS) | BILLINGFullAccess-Policy | Full permissions for Billing Center, Account Center, Cost Center, Enterprise Center, and Message Center. It is generally granted to administrators.                                                                                                                                                                                    |
|                               | BILLINGOperatorPolicy    | Permissions for viewing information in Billing Center, Account Center, Cost Center, Enterprise Center, and Message Center, for example, viewing the change, management, and use of cloud services. This policy does not have financial permissions. It is generally granted to the technical personnel, such as R&D and O&M personnel. |
|                               | BILLINGFinancePolicy     | Permissions for financial operations, including payment, consumption, invoicing, and cost. This policy does not have permission for modifying cloud services. It is generally granted to financial personnel.                                                                                                                          |

| Service                                     | Identity Policy                            | Description                                                                                                                                                        |
|---------------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enterprise Center                           | BusinessUnitCenter-FullAccessPolicy        | Full permissions for Enterprise Center. It is generally granted to the management personnel of an organization.                                                    |
|                                             | BusinessUnitCenter-ReadOnlyPolicy          | Permissions to view data in Enterprise Center. It is generally granted to the members in an enterprise organization.                                               |
|                                             | BusinessUnitCenter-MemberFinanceReadPolicy | Permissions for a master account to view the financial information of its member accounts. It is generally granted to the management personnel of an organization. |
| Enterprise Project Management Service (EPS) | EPSReadOnlyPolicy                          | Read-only permissions for EPS.                                                                                                                                     |
|                                             | EPSFullAccessPolicy                        | Full permissions for EPS.                                                                                                                                          |
| Cost Center                                 | CostCenterFullAccessPolicy                 | Full permissions for Cost Center. Generally, this policy is granted to cost administrators and cost analysis personnel.                                            |
|                                             | CostCenterReadOnlyPolicy                   | Permissions to view data in Cost Center. Generally, this policy is granted to those who want to view cost reports.                                                 |

# 3 Identity Policy-based Authorization

---

## 3.1 Compute

### 3.1.1 Auto Scaling (AS)

IAM provides common system-defined identity policies for services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.

- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by AS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column of an action is empty (-), the action does not support any condition keys.

For details about the condition keys defined by AS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for AS.

**Table 3-1** Actions supported by AS

| Action                 | Description                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                           | Alias            |
|------------------------|----------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| as:scalingGroup:create | Grants permission to create an AS group.     | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">as:ScalingConfigId</a></li> <li>• <a href="#">as:VpcId</a></li> <li>• <a href="#">as:VpcSubnetId</a></li> <li>• <a href="#">as:ElbPoolId</a></li> <li>• <a href="#">as:MaxInstanceSize</a></li> <li>• <a href="#">as:MinInstanceSize</a></li> </ul> | as:groups:create |
| as:scalingGroup:delete | Grants permission to delete an AS group.     | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                                                                                                                      | as:groups:delete |
| as:scalingGroup:list   | Grants permission to list AS groups.         | list         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                   | as:groups:list   |
| as:scalingGroup:get    | Grants permission to query AS group details. | read         | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                                                                                                                      | as:groups:get    |
| as:scalingGroup:update | Grants permission to modify an AS group.     | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">as:ScalingConfigId</a></li> <li>• <a href="#">as:VpcSubnetId</a></li> <li>• <a href="#">as:ElbPoolId</a></li> <li>• <a href="#">as:MaxInstanceSize</a></li> <li>• <a href="#">as:MinInstanceSize</a></li> </ul>                                                                                                                                   | as:groups:update |

| Action                  | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Alias             |
|-------------------------|--------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| as:scalingGroup:resume  | Grants permission to enable an AS group.         | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           | as:groups:action  |
| as:scalingGroup:pause   | Grants permission to disable an AS group.        | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                           | as:groups:action  |
| as:scalingConfig:create | Grants permission to create an AS configuration. | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">as:EcsInstanceId</a></li> <li>• <a href="#">as:EcsInstanceType</a></li> <li>• <a href="#">as:EcsFlavorId</a></li> <li>• <a href="#">as:ImageId</a></li> <li>• <a href="#">as:ImsDiskImageId</a></li> <li>• <a href="#">as:CbrDiskSnapshotId</a></li> <li>• <a href="#">as:EcsServerGroupId</a></li> <li>• <a href="#">as:EvsEncrypted</a></li> <li>• <a href="#">as:KmsKeyId</a></li> <li>• <a href="#">as:EvsVolumeType</a></li> <li>• <a href="#">as:KpsSSHKeyPairName</a></li> <li>• <a href="#">as:AssociatePublicIp</a></li> </ul> | as:configs:create |
| as:scalingConfig:delete | Grants permission to delete an AS configuration. | write        | scalingConfig*              | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | as:configs:delete |

| Action                                    | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                    |
|-------------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| as:scalingConfig:batchDelete              | Grants permission to delete AS configurations.                  | write        | scalingConfig*              | -                                                                                                                                                  | as:configs:batchDelete   |
| as:scalingConfig:list                     | Grants permission to list AS configurations.                    | list         | scalingConfig*              | -                                                                                                                                                  | as:configs:list          |
| as:scalingConfig:get                      | Grants permission to query AS configuration details.            | read         | scalingConfig*              | -                                                                                                                                                  | as:configs:get           |
| as:scalingGroup:batchAddInstances         | Grants permission to add instances to an AS group.              | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instances:batchAction |
| as:scalingGroup:batchRemoveInstances      | Grants permission to delete instances from an AS group.         | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instances:batchAction |
| as:scalingGroup:batchSetInstanceProtect   | Grants permission to enable instance protection for instances.  | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instances:batchAction |
| as:scalingGroup:batchSetInstanceUnprotect | Grants permission to disable instance protection for instances. | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instances:batchAction |

| Action                                      | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|---------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| as:scalingGroup:batchSetInstanceStandby     | Grants permission to put instances into the standby status.    | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instance:batchAction |
| as:scalingGroup:batchSetInstanceExitStandby | Grants permission to move instances out of the standby status. | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instance:batchAction |
| as:scalingGroup:deleteInstance              | Grants permission to delete instances from an AS group.        | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instance:delete      |
| as:scalingGroup:listInstances               | Grants permission to list instances in an AS group.            | list         | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instance:list        |
| as:scalingPolicy:create                     | Grants permission to create an AS policy.                      | write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | as:policies:create      |
| as:scalingPolicy:list                       | Grants permission to list AS policies.                         | list         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | as:policies:list        |
| as:scalingPolicy:get                        | Grants permission to query AS policy details.                  | read         | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | as:policies:get         |



| Action                       | Description                                        | Access Level | Resource Type (*: required) | Condition Key                         | Alias                   |
|------------------------------|----------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------|
| as:scalingPolicy:update      | Grants permission to modify an AS policy.          | write        | -                           | <a href="#">g:EnterpriseProjectId</a> | as:policies:update      |
| as:scalingPolicy:delete      | Grants permission to delete an AS policy.          | write        | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a> | as:policies:delete      |
| as:scalingPolicy:execute     | Grants permission to execute an AS policy.         | write        | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a> | as:policies:action      |
| as:scalingPolicy:resume      | Grants permission to enable an AS policy.          | write        | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a> | as:policies:action      |
| as:scalingPolicy:pause       | Grants permission to disable an AS policy.         | write        | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a> | as:policies:action      |
| as:scalingPolicy:batchPause  | Grants permission to disable AS policies.          | write        | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a> | as:policies:batchAction |
| as:scalingPolicy:batchResume | Grants permission to enable AS policies.           | write        | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a> | as:policies:batchAction |
| as:scalingPolicy:batchDelete | Grants permission to delete AS policies.           | write        | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a> | as:policies:batchAction |
| as:scalingPolicy:listAll     | Grants permission to list AS policies of a tenant. | list         | -                           | <a href="#">g:EnterpriseProjectId</a> | as:policies:list        |

| Action                              | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                           | Alias                     |
|-------------------------------------|------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| as:scalingGroup:listActivityLogs    | Grants permission to query scaling action logs.      | list         | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                      | as:activityLogs:list      |
| as:scalingPolicy:listExecuteLogs    | Grants permission to query AS policy execution logs. | list         | scalingPolicy*              | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                   | as:policyExecuteLogs:list |
| as::tagResource                     | Grants permission to add tags.                       | tagging      | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | as:tags:set               |
| as::untagResource                   | Grants permission to delete tags.                    | tagging      | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | as:tags:set               |
| as::listTags                        | Grants permission to query tags of all resources.    | list         | -                           | -                                                                                                                                                                                       | as:tags:list              |
| as::listTagsForResource             | Grants permission to query tags of a resource.       | list         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                   | as:tags:get               |
| as::listResourcesByTag              | Grants permission to query resources by tag.         | list         | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                  | as:tagResources:list      |
| as:scalingGroup:createLifecycleHook | Grants permission to create a lifecycle hook.        | write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                   | as:lifecycleHooks:create  |

| Action                               | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                    |
|--------------------------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| as:scalingGroup:listLifecycleHooks   | Grants permission to list lifecycle hooks.         | list         | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:lifecycleHooks:list   |
| as:scalingGroup:getLifecycleHook     | Grants permission to query lifecycle hook details. | read         | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:lifecycleHooks:get    |
| as:scalingGroup:updateLifecycleHook  | Grants permission to modify a lifecycle hook.      | write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | as:lifecycleHooks:update |
| as:scalingGroup:deleteLifecycleHook  | Grants permission to delete a lifecycle hook.      | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:lifecycleHooks:delete |
| as:scalingGroup:callbackInstanceHook | Grants permission to call back a lifecycle hook.   | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instanceHooks:action  |
| as:scalingGroup:listInstanceHooks    | Grants permission to query suspended instances.    | list         | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:instanceHooks:list    |
| as:scalingGroup:createNotification   | Grants permission to create notifications.         | write        | scalingGroup*               | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | as:notifications:set     |
| as:scalingGroup:listNotifications    | Grants permission to query notifications.          | list         | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:notifications:list    |

| Action                             | Description                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|------------------------------------|-----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| as:scalingGroup:deleteNotification | Grants permission to delete notifications.                | write        | scalingGroup*               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | as:notifications:delete |
| as:scalingGroup:getQuotas          | Grants permission to query instance and AS policy quotas. | read         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | as:quotas:get           |
| as::listQuotas                     | Grants permission to query instance and AS policy quotas. | read         | -                           | -                                                                                                                                                  | as:quotas:get           |

Each API of AS usually supports one or more actions. [Table 3-2](#) lists the supported actions and dependencies.

**Table 3-2** Actions and dependencies supported by AS APIs

| API                                                                      | Action                 | Dependencies |
|--------------------------------------------------------------------------|------------------------|--------------|
| POST /autoscaling-api/v1/{project_id}/scaling_group                      | as:scalingGroup:create | -            |
| DELETE /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id} | as:scalingGroup:delete | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_group                       | as:scalingGroup:list   | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}    | as:scalingGroup:get    | -            |
| PUT /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}    | as:scalingGroup:update | -            |

| API                                                                                      | Action                                                                                                                                                                                                                                                                                                                                          | Dependencies |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| POST /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}/action            | as:scalingGroup:resume                                                                                                                                                                                                                                                                                                                          | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_group/{scaling_group_id}/action            | as:scalingGroup:pause                                                                                                                                                                                                                                                                                                                           | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_configurationCreateScalingConfig           | as:scalingConfig:create                                                                                                                                                                                                                                                                                                                         | -            |
| DELETE /autoscaling-api/v1/{project_id}/scaling_configuration/{scaling_configuration_id} | as:scalingConfig:delete                                                                                                                                                                                                                                                                                                                         | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_configurations                             | as:scalingConfig:batchDelete                                                                                                                                                                                                                                                                                                                    | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_configuration                               | as:scalingConfig:list                                                                                                                                                                                                                                                                                                                           | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_configuration/{scaling_configuration_id}    | as:scalingConfig:get                                                                                                                                                                                                                                                                                                                            | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_group_instance/{scaling_group_id}/action   | <ul style="list-style-type: none"> <li>as:scalingGroup:batchAddInstances</li> <li>as:scalingGroup:batchSetInstancesProtect</li> <li>as:scalingGroup:batchRemoveInstances</li> <li>as:scalingGroup:batchSetInstancesStandby</li> <li>as:scalingGroup:batchSetInstancesUnprotect</li> <li>as:scalingGroup:batchSetInstancesExitStandby</li> </ul> | -            |
| DELETE /autoscaling-api/v1/{project_id}/scaling_group_instance/{instance_id}             | as:scalingGroup:deleteInstance                                                                                                                                                                                                                                                                                                                  | -            |

| API                                                                                 | Action                                                                                                                                      | Dependencies |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| GET /autoscaling-api/v1/{project_id}/scaling_group_instance/{scaling_group_id}/list | as:scalingGroup:listInstances                                                                                                               | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_policy                                | as:scalingPolicy:create                                                                                                                     | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_group_id}/list         | as:scalingPolicy:list                                                                                                                       | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}             | as:scalingPolicy:get                                                                                                                        | -            |
| PUT /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}             | as:scalingPolicy:update                                                                                                                     | -            |
| DELETE /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}          | as:scalingPolicy:delete                                                                                                                     | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_policy/{scaling_policy_id}/action     | <ul style="list-style-type: none"> <li>as:scalingPolicy:resume</li> <li>as:scalingPolicy:pause</li> <li>as:scalingPolicy:execute</li> </ul> | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_policies/action                       | as:scalingPolicy:batchDelete<br>as:scalingPolicy:batchPause<br>as:scalingPolicy:batchResume                                                 | -            |
| POST /autoscaling-api/v2/{project_id}/scaling_policy                                | as:scalingPolicy:create                                                                                                                     | -            |
| GET /autoscaling-api/v2/{project_id}/scaling_policy                                 | as:scalingPolicy:listAll                                                                                                                    | -            |
| GET /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_resource_id}/list      | as:scalingPolicy:list                                                                                                                       | -            |
| GET /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_policy_id}             | as:scalingPolicy:get                                                                                                                        | -            |
| PUT /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_policy_id}             | as:scalingPolicy:update                                                                                                                     | -            |

| API                                                                                                  | Action                              | Dependencies |
|------------------------------------------------------------------------------------------------------|-------------------------------------|--------------|
| GET /autoscaling-api/v1/{project_id}/scaling_activity_log/{scaling_group_id}                         | as:scalingGroup:listActivityLogs    | -            |
| GET /autoscaling-api/v2/{project_id}/scaling_activity_log/{scaling_group_id}                         | as:scalingGroup:listActivityLogs    | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_policy_execute_log/{scaling_policy_id}                  | as:scalingPolicy:listExecuteLogs    | -            |
| POST /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags/action                      | as::tagResource                     | -            |
| POST /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags/action                      | as::untagResource                   | -            |
| GET /autoscaling-api/v1/{project_id}/{resource_type}/tags                                            | as::listTags                        | -            |
| GET /autoscaling-api/v1/{project_id}/{resource_type}/{resource_id}/tags                              | as::listTagsForResource             | -            |
| POST /autoscaling-api/v1/{project_id}/{resource_type}/resource_instances/action                      | as::listResourcesByTag              | -            |
| POST /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}                      | as:scalingGroup:createLifecycleHook | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/list                  | as:scalingGroup:listLifecycleHooks  | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name} | as:scalingGroup:getLifecycleHook    | -            |

| API                                                                                                     | Action                               | Dependencies |
|---------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| PUT /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name}    | as:scalingGroup:updateLifecycleHook  | -            |
| DELETE /autoscaling-api/v1/{project_id}/scaling_lifecycle_hook/{scaling_group_id}/{lifecycle_hook_name} | as:scalingGroup:deleteLifecycleHook  | -            |
| PUT /autoscaling-api/v1/{project_id}/scaling_instance_hook/{scaling_group_id}/callback                  | as:scalingGroup:callbackInstanceHook | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_instance_hook/{scaling_group_id}/list                      | as:scalingGroup:listInstanceHooks    | -            |
| PUT /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}                            | as:scalingGroup:createNotification   | -            |
| DELETE /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}/{topic_urn}             | as:scalingGroup:deleteNotification   | -            |
| GET /autoscaling-api/v1/{project_id}/scaling_notification/{scaling_group_id}                            | as:scalingGroup:listNotifications    | -            |
| GET /autoscaling-api/v1/{project_id}/quotas/{scaling_group_id}                                          | as:scalingGroup:getQuotas            | -            |
| GET /autoscaling-api/v1/{project_id}/quotas                                                             | as::listQuotas                       | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-3](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all



resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can specify in identity policy statements for AS.

**Table 3-3** Resource types supported by AS

| Resource Type | URN                                                        |
|---------------|------------------------------------------------------------|
| scalingGroup  | as:<region>:<account-id>:scalingGroup:<scaling-group-id>   |
| scalingConfig | as:<region>:<account-id>:scalingConfig:<scaling-config-id> |
| scalingPolicy | as:<region>:<account-id>:scalingPolicy:<scaling-policy-id> |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **as:**) only apply to operations of the AS service. For details, see [Table 3-4](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

The following table lists the condition keys that you can define in identity policies for AS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-4** Service-specific condition keys supported by AS

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                       |
|--------------------------------|---------|-------------------------------|-------------------------------------------------------------------|
| as:ScalingConfigId             | String  | Single-valued                 | Filters access by AS configuration ID.                            |
| as:VpcId                       | String  | Single-valued                 | Filters access by VPC ID.                                         |
| as:VpcSubnetId                 | String  | Multivalued                   | Filters access by subnet ID.                                      |
| as:ElbPoolId                   | String  | Multivalued                   | Filters access by ELB backend server group ID.                    |
| as:MaxInstanceSize             | Integer | Single-valued                 | Filters access by the maximum number of instances in an AS group. |
| as:MinInstancesSize            | Integer | Single-valued                 | Filters access by the minimum number of instances in an AS group. |
| as:EcsInstanceId               | String  | Single-valued                 | Filters access by the ECS ID used for AS configuration creation.  |
| as:EcsInstanceType             | String  | Single-valued                 | Filters access by the spot or pay-per-use billing mode.           |
| as:EcsFlavorId                 | String  | Multivalued                   | Filters access by the flavor ID used for ECS creation.            |
| as:ImageId                     | String  | Single-valued                 | Filters access by the image ID used for ECS creation.             |
| as:ImsDiskImageId              | String  | Multivalued                   | Filters access by the disk image ID used for ECS creation.        |
| as:CbrDiskSnapshotId           | String  | Multivalued                   | Filters access by the disk backup ID used for ECS creation.       |
| as:EcsServerGroupId            | String  | Single-valued                 | Filters access by the ECS group ID used for ECS creation.         |

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                     |
|--------------------------------|---------|-------------------------------|-----------------------------------------------------------------|
| as:EvsEncrypted                | Boolean | Single-valued                 | Filters access based on whether disk encryption is enabled.     |
| as:KmsKeyId                    | String  | Multivalued                   | Filters access by the key ID used for disk encryption.          |
| as:EvsVolumeType               | String  | Multivalued                   | Filters access by the disk type used for ECS creation.          |
| as:KpsSSHKeyPairName           | String  | Single-valued                 | Filters access by the key pair name used for ECS creation.      |
| as:AssociatePublicIp           | Boolean | Single-valued                 | Filters access based on whether auto EIP assignment is enabled. |

### 3.1.2 Bare Metal Server (BMS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by BMS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column of an action is empty (-), the action does not support any condition keys.

For details about the condition keys defined by BMS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for BMS.

**Table 3-5** Actions supported by BMS

| Action                            | Description                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                   | Alias           |
|-----------------------------------|------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| bms:servers:updateBaremetalServer | Grants permission to modify a BMS. | write        | instance*                   | <ul style="list-style-type: none"><li>• <a href="#">g:EnterpriseProjectId</a></li><li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li></ul> | bms:servers:put |

| Action                                              | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias           |
|-----------------------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| bms:servers:showBaremetalServerInterfaceAttachments | Grants permission to query BMS NICs.                                             | read         | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | bms:servers:get |
| bms:servers:resetServerPwd                          | Grants permission to reset a BMS password with a few clicks.                     | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -               |
| bms:servers:showResetPasswordFlag                   | Grants permission to check whether BMS passwords can be reset with a few clicks. | read         | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | bms:servers:get |
| bms:servers:showWindowsBaremetalServerPwd           | Grants permission to obtain Windows BMS passwords.                               | read         | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | bms:servers:get |
| bms:servers:deletePassword                          | Grants permission to delete Windows BMS passwords.                               | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -               |
| bms:servers:showBaremetalServerVolumeInfo           | Grants permission to query EVS disks attached to a BMS.                          | read         | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | bms:servers:get |

| Action             | Description                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Alias |
|--------------------|-----------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| bms:servers:create | Grants permission to create BMSs. | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">bms:FlavorId</a></li> <li>• <a href="#">bms:VpcId</a></li> <li>• <a href="#">bms:SubnetId</a></li> <li>• <a href="#">bms:KmsKeyId</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">bms:ImageId</a></li> <li>• <a href="#">bms:SSHKeyPairName</a></li> <li>• <a href="#">bms:AvailabilityZone</a></li> <li>• <a href="#">bms:VolumeType</a></li> <li>• <a href="#">bms:MetadataOptionsHttpEndpoint</a></li> <li>• <a href="#">bms:MetadataOptionsHttpTokens</a></li> <li>• <a href="#">bms:MetadataAgencyName</a></li> </ul> | -     |

| Action                          | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                         | Alias           |
|---------------------------------|---------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| bms:servers:showBaremetalServer | Grants permission to query details about a BMS.   | read         | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                    | bms:servers:get |
| bms:servers:attachVolume        | Grants permission to attach EVS disks to a BMS.   | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">bms:KmsKeyId</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">bms:VolumeType</a></li> <li>• <a href="#">bms:VolumeId</a></li> </ul> | -               |
| bms:servers:detachVolume        | Grants permission to detach EVS disks from a BMS. | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                    | -               |
| bms:servers:updateMetadata      | Grants permission to update BMS metadata.         | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">bms:MetadataAgencyName</a></li> </ul>                                                                                                                  | -               |

| Action                              | Description                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                     | Alias             |
|-------------------------------------|-----------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| bms:servers:reinstallOS             | Grants permission to reinstall a BMS OS.      | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">bms:KmsKeyId</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">bms:SSHKeyPairName</a></li> </ul> | -                 |
| bms:servers:showBaremetalServerTags | Grants permission to query BMS tags.          | read         | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                | bms: servers: get |
| bms:servers:start                   | Grants permission to start BMSs in a batch.   | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                | -                 |
| bms:servers:reboot                  | Grants permission to restart BMSs in a batch. | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                | -                 |
| bms:servers:stop                    | Grants permission to stop BMSs in a batch.    | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                | -                 |
| bms:servers:list                    | Grants permission to query BMS details.       | list         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                             | -                 |



| Action                                      | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                              | Alias            |
|---------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| bms:serverFlavors:get                       | Grants permission to query flavor details and extended flavor information. | list         | -                           | -                                                                                                                                                                                          | -                |
| bms:serverQuotas:get                        | Grants permission to query tenant quotas.                                  | read         | -                           | -                                                                                                                                                                                          | -                |
| bms:servers:batchCreateBatchMetalServerTags | Grants permission to add tags in a batch.                                  | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>     | bms: servers:put |
| bms:servers:batchDeleteBatchMetalServerTags | Grants permission to delete tags in a batch.                               | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>     | bms: servers:put |
| bms:servers:addNics                         | Grants permission to bind NICs to a BMS.                                   | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">bms:SubnetId</a></li> </ul> | -                |
| bms:server:deleteNics                       | Grants permission to unbind NICs from a BMS.                               | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                         | -                |

| Action                            | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                             | Alias |
|-----------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| bms:servers:serialConsole         | Grants permission to obtain an address for remotely logging in to a BMS. | read         | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                        | -     |
| bms:servers:changeOS              | Grants permission to change a BMS OS.                                    | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">bms:KmsKeyId</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">bms:ImageId</a></li> <li>• <a href="#">bms:SSHPKeyPairName</a></li> </ul> | -     |
| bms:server:updateInterface        | Grants permission to modify BMS NICs.                                    | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                        | -     |
| bms:servers:updateMetadataOptions | Updating BMS metadata                                                    | write        | instance*                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">bms:MetadataOptionsHttpEndpoint</a></li> <li>• <a href="#">bms:MetadataOptionsHttpTokens</a></li> </ul>                                                    | -     |

| Action                          | Description            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias |
|---------------------------------|------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| bms:servers:showMetadataOptions | Obtaining BMS metadata | read         | instance*                   | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

Each API of BMS usually supports one or more actions. [Table 3-6](#) lists the supported actions and dependencies.

**Table 3-6** Actions and dependencies supported by BMS APIs

| API                                                                     | Action                                              | Dependencies |
|-------------------------------------------------------------------------|-----------------------------------------------------|--------------|
| PUT /v1/{project_id}/baremetalservers/{server_id}                       | bms:servers:updateBaremetalServer                   | -            |
| GET /v1/{project_id}/baremetalservers/{server_id}/os-interface          | bms:servers:showBaremetalServerInterfaceAttachments | -            |
| PUT /v1/{project_id}/baremetalservers/{server_id}/os-reset-password     | bms:servers:resetServerPwd                          | -            |
| GET /v1/{project_id}/baremetalservers/{server_id}/os-resetpwd-flag      | bms:servers:showResetPasswordFlag                   | -            |
| GET /v1/{project_id}/baremetalservers/{server_id}/os-server-password    | bms:servers:showWindowsBaremetalServerPwd           | -            |
| DELETE /v1/{project_id}/baremetalservers/{server_id}/os-server-password | bms:servers:deletePassword                          | -            |
| GET /v1/{project_id}/baremetalservers/{server_id}/os-volume_attachments | bms:servers:showBaremetalServerVolumeInfo           | -            |

| API                                                                               | Action                              | Dependencies                                                                                                                                                                       |
|-----------------------------------------------------------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/{project_id}/baremetalservers                                            | bms:servers:create                  | <ul style="list-style-type: none"> <li>eip:publicips:create</li> <li>eip:publicips:associateInstance</li> <li>iam:agencies:pass</li> <li>eip:bandwidths:insertPublicIps</li> </ul> |
| GET /v1/{project_id}/baremetalservers/{server_id}                                 | bms:servers:showBaremetalServer     | -                                                                                                                                                                                  |
| POST /v1/{project_id}/baremetalservers/{server_id}/attachvolume                   | bms:servers:attachVolume            | evs:volumes:use                                                                                                                                                                    |
| DELETE /v1/{project_id}/baremetalservers/{server_id}/detachvolume/{attachment_id} | bms:servers:detachVolume            | -                                                                                                                                                                                  |
| POST /v1/{project_id}/baremetalservers/{server_id}/metadata                       | bms:servers:updateMetadata          | iam:agencies:pass                                                                                                                                                                  |
| POST /v1/{project_id}/baremetalservers/{server_id}/reinstallos                    | bms:servers:reinstallOS             | -                                                                                                                                                                                  |
| GET /v1/{project_id}/baremetalservers/{server_id}/tags                            | bms:servers:showBaremetalServerTags | -                                                                                                                                                                                  |
| POST /v1/{project_id}/baremetalservers/action                                     | bms:servers:start                   | -                                                                                                                                                                                  |
| POST /v1/{project_id}/baremetalservers/action                                     | bms:servers:reboot                  | -                                                                                                                                                                                  |
| POST /v1/{project_id}/baremetalservers/action                                     | bms:servers:stop                    | -                                                                                                                                                                                  |
| GET /v1/{project_id}/baremetalservers/detail                                      | bms:servers:list                    | -                                                                                                                                                                                  |
| GET /v1/{project_id}/baremetalservers/flavors                                     | bms:serverFlavors:get               | -                                                                                                                                                                                  |
| GET /v1/{project_id}/baremetalservers/limits                                      | bms:serverQuotas:get                | -                                                                                                                                                                                  |

| API                                                                      | Action                                     | Dependencies |
|--------------------------------------------------------------------------|--------------------------------------------|--------------|
| POST /v1/{project_id}/baremetalservers/{server_id}/tags/action           | bms:servers:batchCreateBaremetalServerTags | -            |
| POST /v1/{project_id}/baremetalservers/{server_id}/tags/action           | bms:servers:batchDeleteBaremetalServerTags | -            |
| POST /v1/{project_id}/baremetalservers/{server_id}/nics                  | bms:servers:addNics                        | -            |
| POST /v1/{project_id}/baremetalservers/{server_id}/nics/delete           | bms:server:deleteNics                      | -            |
| POST /v1/{project_id}/baremetalservers/{server_id}/remote_console        | bms:servers:serialConsole                  | -            |
| POST /v1/{project_id}/baremetalservers/{server_id}/changeos              | bms:servers:changeOS                       | -            |
| PUT /v1/{project_id}/baremetalservers/{server_id}/os-interface/{port_id} | bms:server:updateInterface                 | -            |
| PUT /v1/{project_id}/baremetalservers/{server_id}/metadata-options       | bms:servers:updateMetadataOptions          | -            |
| GET /v1/{project_id}/baremetalservers/{server_id}/metadata-options       | bms:servers:showMetadataOptions            | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-7](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for BMS.

**Table 3-7** Resource types supported by BMS

| Resource Type | URN                                            |
|---------------|------------------------------------------------|
| instance      | bms:<region>:<account-id>:instance:<server-id> |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **bms:**) only apply to operations of the BMS service. For details, see [Table 3-8](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by BMS

The following table lists the condition keys that you can define in identity policies for BMS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-8** Service-specific condition keys supported by BMS

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                |
|--------------------------------|--------|-------------------------------|----------------------------------------------------------------------------|
| bms:KmsKeyId                   | string | Multivalued                   | Filters access based on the KMS key ID specified in the request parameter. |

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                                       |
|--------------------------------|--------|-------------------------------|-------------------------------------------------------------------------------------------------------------------|
| bms:FlavorId                   | string | Multivalued                   | Filters access based on the flavor ID specified in the request parameter.                                         |
| bms:VpcId                      | string | Multivalued                   | Filters access based on the VPC ID specified in the request parameter.                                            |
| bms:SubnetId                   | string | Multivalued                   | Filters access based on the subnet ID specified in the request parameter.                                         |
| bms:ImageId                    | string | Single-valued                 | Filters access based on the image ID specified in the request parameter.                                          |
| bms:SSHKeyPair Name            | string | Single-valued                 | Filters access based on the key name specified in the request parameter.                                          |
| bms:Availability Zone          | string | Single-valued                 | Filters access based on the availability zone specified in the request parameter.                                 |
| bms:VolumeType                 | string | Multivalued                   | Filters access based on the EVS disk type specified in the request parameter.                                     |
| bms:VolumeId                   | string | Single-valued                 | Filters access based on the volume ID specified in the request parameter.                                         |
| bms:MetadataOptionsHttpTokens  | string | Single-valued                 | Filters access based on the <b>http_tokens</b> parameter in the <b>metadata-options</b> structure in the request. |

| Service-specific Condition Key  | Type   | Single-valued/<br>Multivalued | Description                                                                                                         |
|---------------------------------|--------|-------------------------------|---------------------------------------------------------------------------------------------------------------------|
| bms:MetadataAgencyName          | string | Single-valued                 | Filters access based on the <b>agency_name</b> parameter in the <b>metadata</b> structure in the request.           |
| bms:MetadataOptionsHttpEndpoint | string | Single-valued                 | Filters access based on the <b>http_endpoint</b> parameter in the <b>metadata-options</b> structure in the request. |

### 3.1.3 Elastic Cloud Server (ECS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.



- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by ECS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by ECS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for ECS.

**Table 3-9** Actions supported by ECS

| Action                         | Description                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Alias                   |
|--------------------------------|-----------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| ecs:cloudServers:createServers | Grants permission to create ECSs. | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">ecs:imageId</a></li> <li>• <a href="#">ecs:FlavorId</a></li> <li>• <a href="#">ecs:VpcId</a></li> <li>• <a href="#">ecs:SubnetId</a></li> <li>• <a href="#">ecs:PortId</a></li> <li>• <a href="#">ecs:KmsKeyId</a></li> <li>• <a href="#">ecs:AvailabilityZone</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">cbr:VaultId</a></li> <li>• <a href="#">ecs:SSHKeyPairName</a></li> <li>• <a href="#">ecs:SupportAgentType</a></li> <li>• <a href="#">ecs:ImageSupportAgentType</a></li> <li>• <a href="#">ecs:ImageType</a></li> <li>• <a href="#">ecs:OsVersion</a></li> <li>• <a href="#">ecs:OsType</a></li> <li>• <a href="#">ecs:ImagePlatform</a></li> </ul> | ecs:cloudServers:create |
| ecs:cloudServers:deleteServers | Grants permission to delete ECSs. | write        | instance*                   | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ecs:cloudServers:delete |

| Action                                   | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                              | Alias                |
|------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| ecs:cloudServers:resize                  | Grants permission to modify ECS specifications.                                 | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">ecs:FlavorId</a></li> </ul> | -                    |
| ecs:cloudServers:attachSharedVolume      | Grants permission to attach a specified EVS disk to multiple ECSs in a batch.   | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">ecs:KmsKeyId</a></li> <li>• <a href="#">ecs:VolumeId</a></li> </ul>                          | -                    |
| ecs:cloudServers:showServer              | Grants permission to query ECS details.                                         | read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                         | ecs:cloudServers:get |
| ecs:cloudServers:attach                  | Grants permission to attach disks to an ECS.                                    | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">ecs:KmsKeyId</a></li> <li>• <a href="#">ecs:VolumeId</a></li> </ul>                          | -                    |
| ecs:cloudServers:showServerBlockDevice   | Grants permission to query information about a single disk attached to an ECS.  | read         | instance *                  | -                                                                                                                                                                                          | ecs:cloudServers:get |
| ecs:cloudServers:updateServerBlockDevice | Grants permission to modify information about a single disk attached to an ECS. | write        | instance *                  | -                                                                                                                                                                                          | ecs:cloudServers:put |

| Action                                | Description                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                       | Alias                |
|---------------------------------------|------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| ecs:cloudServers:changeOS             | Grants permission to change the ECS OS.        | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">ecs:imageID</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">ecs:KmsKeyId</a></li> <li>• <a href="#">ecs:SSHKeyPairName</a></li> <li>• <a href="#">ecs:ImageType</a></li> <li>• <a href="#">ecs:OsVersion</a></li> <li>• <a href="#">ecs:OsType</a></li> <li>• <a href="#">ecs:ImagePlatform</a></li> </ul> | -                    |
| ecs:cloudServers:detachVolume         | Grants permission to detach disks from an ECS. | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                                                                                  | -                    |
| ecs:cloudServers:updateMetadata       | Grants permission to update ECS metadata.      | write        | instance *                  | -                                                                                                                                                                                                                                                                                                                                                                                   | -                    |
| ecs:cloudServers:deleteMetadata       | Grants permission to delete ECS metadata.      | write        | instance *                  | -                                                                                                                                                                                                                                                                                                                                                                                   | -                    |
| ecs:cloudServers:migrate              | Grants permission to cold migrate ECSs.        | write        | instance *                  | -                                                                                                                                                                                                                                                                                                                                                                                   | -                    |
| ecs:cloudServers:listServerInterfaces | Grants permission to query NICs of an ECS.     | list         | instance *                  | -                                                                                                                                                                                                                                                                                                                                                                                   | ecs:cloudServers:get |

| Action                                       | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                           | Alias                |
|----------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| ecs:cloudServers:showResetPasswordFlag       | Grants permission to query whether one-click password reset is supported. | read         | instance *                  | -                                                                                                                                                       | ecs:cloudServers:get |
| ecs:cloudServers:showServerPassword          | Grants permission to get the password for logging in to an ECS.           | read         | instance *                  | -                                                                                                                                                       | ecs:cloudServers:get |
| ecs:cloudServers:deletePassword              | Grants permission to delete the password for logging in to an ECS.        | write        | instance *                  | -                                                                                                                                                       | -                    |
| ecs:cloudServers:listServerVolumeAttachments | Grants permission to query disks attached to an ECS.                      | list         | instance *                  | -                                                                                                                                                       | ecs:cloudServers:get |
| ecs:cloudServers:rebuild                     | Grants permission to reinstall the ECS OS.                                | write        | instance *                  | <ul style="list-style-type: none"> <li>• evs:Encrypted</li> <li>• <a href="#">ecs:KmsKeyId</a></li> <li>• <a href="#">ecs:SSHKeyPairName</a></li> </ul> | -                    |
| ecs:cloudServers:vnc                         | Grants permission to obtain the VNC login address.                        | read         | instance *                  | -                                                                                                                                                       | -                    |
| ecs:cloudServers:updateServer                | Grants permission to modify ECS information.                              | write        | instance *                  | -                                                                                                                                                       | ecs:cloudServers:put |

| Action                                 | Description                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias                                                                                                                   |
|----------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| ecs:cloudServers:setAutoTerminateTime  | Grants permission to set the automatic destruction time of an ECS. | write        | instance *                  | -                                                                                                                                     | -                                                                                                                       |
| ecs:cloudServers:addNics               | Grants permission to add NICs to an ECS in a batch.                | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">ecs:SubnetId</a></li> <li>• <a href="#">ecs:PortId</a></li> </ul>                | -                                                                                                                       |
| ecs:cloudServerNics:delete             | Grants permission to delete NICs from an ECS in a batch.           | write        | instance *                  | -                                                                                                                                     | -                                                                                                                       |
| ecs:cloudServers:showServerTags        | Grants permission to query ECS tags.                               | list         | instance *                  | -                                                                                                                                     | ecs:cloudServers:get                                                                                                    |
| ecs:cloudServers:batchCreateServerTags | Grants permission to add tags to an ECS in a batch.                | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>• ecs:cloudServers:put</li> <li>• ecs:cloudServers:batchSetServerTags</li> </ul> |
| ecs:cloudServers:batchDeleteServerTags | Grants permission to delete tags from an ECS in a batch.           | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>• ecs:cloudServers:put</li> <li>• ecs:cloudServers:batchSetServerTags</li> </ul> |

| Action                                  | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                | Alias                      |
|-----------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|------------------------------|----------------------------|
| ecs:cloudServers:start                  | Grants permission to start ECSs in a batch.                                 | write        | instance *                  | -                            | -                          |
| ecs:cloudServers:stop                   | Grants permission to stop ECSs in a batch.                                  | write        | instance *                  | -                            | -                          |
| ecs:cloudServers:reboot                 | Grants permission to restart ECSs in a batch.                               | write        | instance *                  | -                            | -                          |
| ecs:cloudServers:batchUpdateServersName | Grants permission to modify ECS information in a batch.                     | write        | instance *                  | -                            | ecs:cloudServers:put       |
| ecs:cloudServers:listServersDetails     | Grants permission to list ECS details.                                      | list         | -                           | <i>g:EnterpriseProjectId</i> | ecs:cloudServers:list      |
| ecs:cloudServerFlavors:get              | Grants permission to query specifications and expansion details about ECSs. | read         | -                           | -                            | -                          |
| ecs:cloudServerQuotas:get               | Grants permission to query tenant quotas.                                   | read         | -                           | -                            | -                          |
| ecs:cloudServers:updateServerInterface  | Grants permission to update NICs of an ECS.                                 | write        | instance *                  | -                            | ecs:cloudServerNics:update |

| Action                                   | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                | Alias                   |
|------------------------------------------|-----------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| ecs:cloudServers:resetServerPwd          | Grants permission to reset the password of an ECS.  | write        | instance *                  | <ul style="list-style-type: none"> <li><i>g:ResourceTag/&lt;tag-key&gt;</i></li> <li><i>g:EnterpriseProjectId</i></li> </ul> | -                       |
| ecs:cloudServers:listServerGroups        | Grants permission to list ECS groups.               | list         | -                           | -                                                                                                                            | ecs:cloudServers:list   |
| ecs:cloudServers:createServerGroup       | Grants permission to create ECS groups.             | write        | -                           | -                                                                                                                            | ecs:cloudServers:create |
| ecs:cloudServers:showServerGroup         | Grants permission to query ECS groups.              | read         | -                           | -                                                                                                                            | ecs:cloudServers:get    |
| ecs:cloudServers:deleteServerGroup       | Grants permission to delete ECS groups.             | write        | -                           | -                                                                                                                            | ecs:cloudServers:delete |
| ecs:cloudServers:addServerGroupMember    | Grants permission to add ECSs to an ECS group.      | write        | -                           | -                                                                                                                            | ecs:cloudServers:create |
| ecs:cloudServers:deleteServerGroupMember | Grants permission to delete ECSs from an ECS group. | write        | -                           | -                                                                                                                            | ecs:cloudServers:delete |
| ecs:cloudServers:listServersByTag        | Grants permission to list ECSs by tag.              | list         | -                           | -                                                                                                                            | ecs:cloudServers:list   |
| ecs:cloudServers:listResizeFlavors       | Grants permission to list supported flavor changes. | list         | -                           | -                                                                                                                            | ecs:cloudServers:list   |



| Action                             | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                               | Alias                 |
|------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| ecs:cloudServers:listServerTags    | Grants permission to list project tags.                                      | list         | -                           | -                                                                                                                                                           | ecs:cloudServers:list |
| ecs:cloudServers:changeVpc         | Grants permission to change the VPC of an ECS.                               | write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">ecs:VpcId</a></li> <li>• <a href="#">ecs:SubnetId</a></li> <li>• <a href="#">ecs:PortId</a></li> </ul> | -                     |
| ecs:cloudServers:changeChargeMode  | Grants permission to change the billing mode of an ECS.                      | write        | instance *                  | -                                                                                                                                                           | -                     |
| ecs:instanceScheduledEvents:list   | Grants permission to list scheduled events.                                  | list         | -                           | -                                                                                                                                                           | -                     |
| ecs:instanceScheduledEvents:accept | Grants permission to accept and authorize the execution of scheduled events. | write        | -                           | -                                                                                                                                                           | -                     |
| ecs:instanceScheduledEvents:update | Grants permission to update scheduled events.                                | write        | -                           | -                                                                                                                                                           | -                     |
| ecs:launchTemplateVersions:list    | Grants permission to list launch template versions.                          | list         | -                           | -                                                                                                                                                           | -                     |
| ecs:launchTemplates:list           | Grants permission to list launch templates.                                  | list         | -                           | -                                                                                                                                                           | -                     |

| Action                            | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ecs:launchTemplates:delete        | Grants permission to delete launch templates.                                   | write        | -                           | -             | -     |
| ecs:launchTemplates:create        | Grants permission to create launch templates.                                   | write        | -                           | -             | -     |
| ecs:cloudservers:redeploy         | Grants permission to redeploy ECSs.                                             | write        | instance *                  | -             | -     |
| ecs:cloudServers:getAutoRecovery  | Grants permission to query whether automatic recovery is configured for an ECS. | read         | instance *                  | -             | -     |
| ecs:cloudServers:setAutoRecovery  | Grants permission to configure automatic recovery for an ECS.                   | write        | instance *                  | -             | -     |
| ecs:cloudServers:triggerCrashDump | Grants permission to trigger crash dump.                                        | write        | instance *                  | -             | -     |
| ecs:recycleBin:updatePolicy       | Grants permission to update the recycle bin policy.                             | write        | -                           | -             | -     |
| ecs:recycleBin:update             | Grants permission to update the recycle bin configuration.                      | write        | -                           | -             | -     |

| Action                               | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|--------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| ecs:recycleBin:get                   | Grants permission to query the recycle bin configuration.                    | read         | -                           | -                                                                                                              | -     |
| ecs:recycleBin:listServers           | Grants permission to list ECSs in the recycle bin.                           | list         | -                           | -                                                                                                              | -     |
| ecs:recycleBin:revertServer          | Grants permission to recover ECSs from the recycle bin.                      | write        | -                           | -                                                                                                              | -     |
| ecs:recycleBin:deleteServer          | Grants permission to delete ECSs from the recycle bin.                       | write        | -                           | -                                                                                                              | -     |
| ecs:metrics:use                      | Grants permission to add an ECS to the monitoring list using the native API. | write        | -                           | ecs:LegacyAPIFlavor                                                                                            | -     |
| ecs:limits:manage                    | Grants permission to query tenant quota limits using the native API.         | write        | -                           | ecs:LegacyAPIFlavor                                                                                            | -     |
| ecs:cloudServers:showMetadataOptions | Grants permission to configure ECS metadata.                                 | read         | -                           | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |

| Action                                 | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| ecs:cloudServers:updateMetadataOptions | Grants permission to update ECS metadata configurations. | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

Each API of ECS usually supports one or more actions. [Table 3-10](#) lists the supported actions and dependencies.

**Table 3-10** Actions and dependencies supported by ECS APIs

| API                                                         | Action                              | Dependencies                                                                                                                                                                               |
|-------------------------------------------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.1/{project_id}/cloudservers                        | ecs:cloudServers:createServers      | <ul style="list-style-type: none"> <li>• eip:publicIps:create</li> <li>• eip:publicIps:associateInstance</li> <li>• iam:agencies:pass</li> <li>• eip:bandwidths:insertPublicIps</li> </ul> |
| POST /v1/{project_id}/cloudservers                          | ecs:cloudServers:createServers      | <ul style="list-style-type: none"> <li>• eip:publicIps:create</li> <li>• eip:publicIps:associateInstance</li> <li>• iam:agencies:pass</li> <li>• eip:bandwidths:insertPublicIps</li> </ul> |
| POST /v1/{project_id}/cloudservers/delete                   | ecs:cloudServers:deleteServers      | -                                                                                                                                                                                          |
| POST /v1.1/{project_id}/cloudservers/{server_id}/resize     | ecs:cloudServers:resize             | -                                                                                                                                                                                          |
| POST /v1/{project_id}/batchaction/attachvolumes/{volume_id} | ecs:cloudServers:attachSharedVolume | evs:volumes:use                                                                                                                                                                            |

| API                                                                       | Action                                   | Dependencies           |
|---------------------------------------------------------------------------|------------------------------------------|------------------------|
| GET /v1/{project_id}/cloudservers/{server_id}                             | ecs:cloudServers:showServer              | -                      |
| GET /v1/{project_id}/cloudservers/{server_id}/os-interface_extension      | ecs:cloudServers:showServer              | -                      |
| GET /v1/{project_id}/cloudservers/{server_id}/appendvolumequota           | ecs:cloudServers:showServer              | -                      |
| POST /v1/{project_id}/cloudservers/{server_id}/attachvolume               | ecs:cloudServers:attach                  | evs:volumes:use        |
| GET /v1/{project_id}/cloudservers/{server_id}/block_device                | ecs:cloudServers:listServerBlockDevices  | -                      |
| GET /v1/{project_id}/cloudservers/{server_id}/block_device/{volume_id}    | ecs:cloudServers:showServerBlockDevice   | -                      |
| PUT /v1/{project_id}/cloudservers/{server_id}/block_device/{volume_id}    | ecs:cloudServers:updateServerBlockDevice | -                      |
| POST /v1/{project_id}/cloudservers/{server_id}/changeos                   | ecs:cloudServers:changeOS                | -                      |
| DELETE /v1/{project_id}/cloudservers/{server_id}/detachvolume/{volume_id} | ecs:cloudServers:detachVolume            | -                      |
| POST /v1/{project_id}/batchaction/detachvolumes/{volume_id}               | ecs:cloudServers:detachVolume            | -                      |
| POST /v1/{project_id}/cloudservers/{server_id}/metadata                   | ecs:cloudServers:updateMetadata          | iam:agencies:pass data |
| DELETE /v1/{project_id}/cloudservers/{server_id}/metadata/{key}           | ecs:cloudServers:deleteMetadata          | -                      |
| POST /v1/{project_id}/cloudservers/{server_id}/migrate                    | ecs:cloudServers:migrate                 | -                      |

| API                                                                 | Action                                       | Dependencies |
|---------------------------------------------------------------------|----------------------------------------------|--------------|
| GET /v1/{project_id}/cloudservers/{server_id}/os-interface          | ecs:cloudServers:listServerInterfaces        | -            |
| PUT /v1/{project_id}/cloudservers/{server_id}/os-reset-password     | ecs:cloudServers:resetServerPwd              | -            |
| GET /v1/{project_id}/cloudservers/{server_id}/os-resetpwd-flag      | ecs:cloudServers:showResetPasswordFlag       | -            |
| GET /v1/{project_id}/cloudservers/{server_id}/os-server-password    | ecs:cloudServers:showServerPassword          | -            |
| DELETE /v1/{project_id}/cloudservers/{server_id}/os-server-password | ecs:cloudServers:deletePassword              | -            |
| GET /v1/{project_id}/cloudservers/{server_id}/os-volume_attachments | ecs:cloudServers:listServerVolumeAttachments | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/reinstall            | ecs:cloudServers:rebuild                     | -            |
| POST /v2/{project_id}/cloudservers/{server_id}/reinstall            | ecs:cloudServers:rebuild                     | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/remote_console       | ecs:cloudServers:vnc                         | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/resize               | ecs:cloudServers:resize                      | -            |
| POST /v1/{project_id}/cloudservers/batch-resize                     | ecs:cloudServers:resize                      | -            |

| API                                                                                                                                                                                                                                      | Action                                 | Dependencies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------|
| GET /v1/{project_id}/cloudservers/detail?flavor={flavor}&name={name}&status={status}&limit={limit}&offset={offset}&not-tags={not-tags}&reservation_id={reservation_id}&enterprise_project_id={enterprise_project_id}&tags={tags}&ip={ip} | ecs:cloudServers:listServersDetails    | -            |
| GET /v1.1/{project_id}/cloudservers/detail                                                                                                                                                                                               | ecs:cloudServers:listServersDetails    | -            |
| GET /v1/{project_id}/availability-zones                                                                                                                                                                                                  | ecs:cloudServers:listServersDetails    | -            |
| PUT /v1/{project_id}/cloudservers/{server_id}                                                                                                                                                                                            | ecs:cloudServers:updateServer          | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/actions/update-auto-terminate-time                                                                                                                                                        | ecs:cloudServers:setAutoTerminateTime  | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/nics                                                                                                                                                                                      | ecs:cloudServers:addNics               | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/nics/delete                                                                                                                                                                               | ecs:cloudServerNics:delete             | -            |
| GET /v1/{project_id}/cloudservers/{server_id}/tags                                                                                                                                                                                       | ecs:cloudServers:showServerTags        | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/tags/action                                                                                                                                                                               | ecs:cloudServers:batchCreateServerTags | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/tags/action                                                                                                                                                                               | ecs:cloudServers:batchDeleteServerTags | -            |
| POST /v1/{project_id}/cloudservers/action                                                                                                                                                                                                | ecs:cloudServers:start                 | -            |
| POST /v1/{project_id}/cloudservers/action                                                                                                                                                                                                | ecs:cloudServers:stop                  | -            |
| POST /v1/{project_id}/cloudservers/action                                                                                                                                                                                                | ecs:cloudServers:reboot                | -            |

| API                                                                                                                                                        | Action                                   | Dependencies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|--------------|
| GET /v1/{project_id}/cloudservers/flavors?availability_zone={availability_zone}&flavor_id={flavor_id}&limit={limit}&marker={marker}                        | ecs:cloudServerFlavors:get               | -            |
| GET /v1/{project_id}/cloudservers/limits                                                                                                                   | ecs:cloudServerQuotas:get                | -            |
| PUT /v1/{project_id}/cloudservers/os-reset-passwords                                                                                                       | ecs:cloudServers:resetServerPwd          | -            |
| GET /v1/{project_id}/cloudservers/os-server-groups?limit={limit}&marker={marker}                                                                           | ecs:cloudServers:listServerGroups        | -            |
| POST /v1/{project_id}/cloudservers/os-server-groups                                                                                                        | ecs:cloudServers:createServerGroup       | -            |
| GET /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}                                                                                       | ecs:cloudServers:showServerGroup         | -            |
| DELETE /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}                                                                                    | ecs:cloudServers:deleteServerGroup       | -            |
| POST /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}/action                                                                               | ecs:cloudServers:addServerGroupMember    | -            |
| POST /v1/{project_id}/cloudservers/os-server-groups/{server_group_id}/action                                                                               | ecs:cloudServers:deleteServerGroupMember | -            |
| GET /v1/{project_id}/cloudservers/resize_flavors?instance_uuid={instance_uuid}&source_flavor_id={source_flavor_id}&source_flavor_name={source_flavor_name} | ecs:cloudServers:listResizeFlavors       | -            |
| GET /v1/{project_id}/cloudservers/tags                                                                                                                     | ecs:cloudServers:listServerTags          | -            |



| API                                                                  | Action                                  | Dependencies                                                                                                |
|----------------------------------------------------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/cloudservers/{server_id}/changeos              | ecs:cloudServers:changeOS               | -                                                                                                           |
| PUT /v1/{project_id}/cloudservers/server-name                        | ecs:cloudServers:batchUpdateServersName | -                                                                                                           |
| POST /v1/{project_id}/cloudservers/resource_instances/action         | ecs:cloudServers:listServersByTag       | -                                                                                                           |
| PUT /v1/{project_id}/cloudservers/{server_id}/os-interface/{port_id} | ecs:cloudServers:updateServerInterface  | -                                                                                                           |
| POST /v1/{project_id}/cloudservers/{server_id}/changevpc             | ecs:cloudServers:changeVpc              | -                                                                                                           |
| POST /v1/{project_id}/cloudservers/actions/change-charge-mode        | ecs:cloudServers:changeChargeMode       | <ul style="list-style-type: none"> <li>• billing:order:pay</li> <li>• billing:subscription:renew</li> </ul> |
| GET /v3/{project_id}/instance-scheduled-events                       | ecs:instanceScheduledEvents:list        | -                                                                                                           |
| POST /v3/{project_id}/instance-scheduled-events/{id}/actions/accept  | ecs:instanceScheduledEvents:accept      | -                                                                                                           |
| PUT /v3/{project_id}/instance-scheduled-events/{id}                  | ecs:instanceScheduledEvents:update      | -                                                                                                           |
| GET /v3/{project_id}/launch-template-versions                        | ecs:launchTemplateVersions:list         | -                                                                                                           |
| GET /v3/{project_id}/launch-templates                                | ecs:launchTemplates:list                | -                                                                                                           |
| DELETE /v2/{domain_id}/auto-launch-groups/{auto_launch_group_id}     | ecs:launchTemplates:delete              | -                                                                                                           |
| POST /v3/{project_id}/launch-templates                               | ecs:launchTemplates:create              | -                                                                                                           |
| POST /v1/{project_id}/cloudservers/{server_id}/actions/redeploy      | ecs:cloudservers:redploy                | -                                                                                                           |

| API                                                                          | Action                                 | Dependencies |
|------------------------------------------------------------------------------|----------------------------------------|--------------|
| GET /v1/{project_id}/cloudservers/flavor-sell-policies?flavor_id={flavor_id} | ecs:cloudServerFlavors:get             | -            |
| GET /v1/{project_id}/cloudservers/flavors/{flavor_id}/resources              | ecs:cloudServerFlavors:get             | -            |
| GET /v1/{project_id}/cloudservers/{server_id}/autorecovery                   | ecs:cloudServers:getAutoRecovery       | -            |
| PUT /v1/{project_id}/cloudservers/{server_id}/autorecovery                   | ecs:cloudServers:setAutoRecovery       | -            |
| POST /v1/{project_id}/cloudservers/{server_id}/actions/trigger-crash-dump    | ecs:cloudServers:triggerCrashDump      | -            |
| PUT /v1/{project_id}/recycle-bin/policy                                      | ecs:recycleBin:updatePolicy            | -            |
| PUT /v1/{project_id}/recycle-bin                                             | ecs:recycleBin:update                  | -            |
| GET /v1/{project_id}/recycle-bin                                             | ecs:recycleBin:get                     | -            |
| POST /v1/{project_id}/recycle-bin/cloudservers/{server_id}/actions/revert    | ecs:recycleBin:revertServer            | -            |
| DELETE /v1/{project_id}/recycle-bin/cloudservers/{server_id}                 | ecs:recycleBin:deleteServer            | -            |
| GET /v1/{project_id}/recycle-bin/cloudservers                                | ecs:recycleBin:listServers             | -            |
| GET /v1/{project_id}/cloudservers/{server_id}/metadata-options               | ecs:cloudServers:showMetadataOptions   | -            |
| PUT /v1/{project_id}/cloudservers/{server_id}/metadata-options               | ecs:cloudServers:updateMetadataOptions | -            |
| GET /v2.1/{project_id}/limits?project_id={project_id}                        | ecs:limits:manage                      | -            |
| POST /v1.0/servers/{server_id}/action                                        | ecs:metrics:use                        | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-11](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for ECS.

**Table 3-11** Resource types supported by ECS

| Resource Type | URN                                            |
|---------------|------------------------------------------------|
| instance      | ecs:<region>:<account-id>:instance:<server-id> |

## Conditions

### About condition keys

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, ecs:) only apply to operations of the ECS service. For details, see [Table 3-12](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition Operators](#).

### Service-specific condition keys supported by ECS

The following table lists the condition keys that you can define in identity policies for ECS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-12** Service-specific condition keys supported by ECS

| Condition Key        | Type   | Single-valued/<br>Multivalued | Description                                                                       |
|----------------------|--------|-------------------------------|-----------------------------------------------------------------------------------|
| ecs:imageId          | string | Multivalued                   | Filters access based on the image ID specified in the request parameter.          |
| ecs:FlavorId         | string | Multivalued                   | Filters access based on the flavor ID specified in the request parameter.         |
| ecs:VpcId            | string | Multivalued                   | Filters access based on the VPC ID specified in the request parameter.            |
| ecs:SubnetId         | string | Multivalued                   | Filters access based on the subnet ID specified in the request parameter.         |
| ecs:KmsKeyId         | string | Multivalued                   | Filters access based on the KMS key ID specified in the request parameter.        |
| ecs:ServerId         | string | Single-valued                 | Filters access based on ECS ID.                                                   |
| ecs:SSHKeyPair Name  | string | Single-valued                 | Filters access based on the SSH key pair name specified in the request parameter. |
| ecs:AvailabilityZone | string | Single-valued                 | Filters access based on the AZ name specified in the request parameter.           |
| ecs:PortId           | string | Multivalued                   | Filters access based on the port ID specified in the request parameter.           |
| ecs:SupportAgentType | string | Multivalued                   | Filters access based on the agent type specified in the request parameter.        |

| Condition Key             | Type   | Single-valued/<br>Multivalued | Description                                                                                                                                                 |
|---------------------------|--------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ecs:ImageSupportAgentType | string | Multivalued                   | Filters access based on the supported image agent type in the request parameter.                                                                            |
| ecs:VolumeId              | string | Single-valued                 | Filters access based on the volume ID specified in the request parameter.                                                                                   |
| ecs:ImageType             | string | Single-valued                 | Filters access based on the image type specified in the request parameter, for example, public images, private images, shared images, or KooGallery images. |
| ecs:OsType                | string | Single-valued                 | Filters access based on the OS type of the image specified in the request parameter, for example, Linux or Windows.                                         |
| ecs:OsVersion             | string | Single-valued                 | Filters access based on the OS version of the image specified in the request, for example, CentOS 7.3 64bit.                                                |
| ecs:ImagePlatform         | string | Single-valued                 | Filters access based on the platform of the image specified in the request, for example, Windows, Ubuntu, Red Hat, SUSE or CentOS.                          |
| ecs:LegacyAPIFlavor       | string | Single-valued                 | Filters access based on the API type. Currently, only native OpenStack APIs are supported.                                                                  |

### 3.1.4 Image Management Service (IMS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN for the Resource element in your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by IMS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column of an action is empty (-), the action does not support any condition keys.

For details about the condition keys defined by IMS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for IMS.

**Table 3-13** Supported Actions

| Action                                                                                                                                                                                                                                                                                                      | Description                             | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                              | Alias           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| ims:images:list                                                                                                                                                                                                                                                                                             | Viewing images                          | list                  | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                      | -               |
| ims:images:get                                                                                                                                                                                                                                                                                              | Viewing details about a specified image | read                  | image *                     | -                                                                                                                                                                                          | -               |
| ims:images:create                                                                                                                                                                                                                                                                                           | Creating image metadata                 | write                 | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>                                                          | -               |
| ims:images:share<br><b>NOTE</b><br>The action <b>ims:images:share</b> is not recommended. Instead, the following actions are recommended for sharing images: <ul style="list-style-type: none"> <li>ims:images:addMember</li> <li>ims:images:deleteMember</li> <li>ims:images:updateMemberStatus</li> </ul> | Sharing images                          | permission_management | image *                     | <ul style="list-style-type: none"> <li><a href="#">ims:TargetOrgPaths</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -               |
| ims:images:copyInRegion                                                                                                                                                                                                                                                                                     | Replicating images within a region      | write                 | image *                     | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">ims:Encrypted</a></li> </ul>      | ims:images:copy |

| Action                     | Description                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Alias           |
|----------------------------|-----------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| ims:images:copyCrossRegion | Replicating images across regions | write        | image *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">ims:Region</a></li> <li>• <a href="#">ims:VaultId</a></li> <li>• <a href="#">g:RequestedRegion</a></li> </ul>                                                                                                                                                                                       | ims:images:copy |
| ims:quotas:get             | Querying the image quota          | read         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -               |
| ims:images:upload          | Uploading images                  | write        | image *                     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -               |
| ims:wholeimages:create     | Creating full-ECS images          | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">ims:Encrypted</a></li> <li>• <a href="#">ims:OriginBucketOrgPaths</a></li> <li>• <a href="#">ims:SourceAvailabilityZone</a></li> <li>• <a href="#">ims:InstanceId</a></li> <li>• <a href="#">ims:VaultId</a></li> <li>• <a href="#">ims:BackupId</a></li> </ul> | -               |
| ims:images:export          | Exporting images                  | read         | image *                     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | -               |



| Action                  | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                               | Alias             |
|-------------------------|-----------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| ims:dataimages:create   | Creating data disk images from external image files | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                                                                                                                      | -                 |
| ims:serverimages:create | Creating images                                     | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">ims:Encrypted</a></li> <li>• <a href="#">ims:OriginBucketOrgPaths</a></li> <li>• <a href="#">ims:SourceAvailabilityZone</a></li> <li>• <a href="#">ims:InstanceId</a></li> <li>• <a href="#">ims:VolumeId</a></li> </ul> | -                 |
| ims:images:setTags      | Updating image tags                                 | tagging      | image *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                                                                                                                                                                       | ims:images:update |
| ims:images:getTags      | Querying image tags                                 | read         | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                                                                                                                      | ims:images:list   |
| ims:images:deleteImage  | Deleting images                                     | write        | image *                     | -                                                                                                                                                                                                                                                                                                                                                                                                                           | ims:images:update |
| ims:images:updateImage  | Updating image information                          | write        | image *                     | -                                                                                                                                                                                                                                                                                                                                                                                                                           | -                 |

| Action                        | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                    | Alias            |
|-------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| ims:images:listOsVersion      | Querying OSs supported by images                                          | list         | -                           | -                                                                                                                                                                                                | ims:images:list  |
| ims:images:getJob             | Querying progresses of asynchronous tasks                                 | read         | -                           | -                                                                                                                                                                                                | ims:images:list  |
| ims:images:import             | Importing images                                                          | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>           | -                |
| ims:images:setOrDeleteTags    | Adding or deleting image tags in a batch                                  | write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                            | -                |
| ims:images:updateMemberStatus | Updating the status of members who can use shared images                  | write        | image *                     | <a href="#">g:RequestTag/&lt;tag-key&gt;</a>                                                                                                                                                     | ims:images:share |
| ims:images:addMember          | Adding a tenant that can use a shared image                               | write        | image *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">ims:TargetOrgPaths</a></li> </ul> | ims:images:share |
| ims:images:deleteMember       | Deleting a tenant from the group where the members can use a shared image | write        | image *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                               | ims:images:share |
| ims:images:listImagesByTag    | Querying images by tag                                                    | read         | -                           | -                                                                                                                                                                                                | ims:images:list  |

| Action                   | Description               | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias           |
|--------------------------|---------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-----------------|
| ims:images:showImageTags | Querying tags of an image | read         | image *                     | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | ims:images:list |
| ims:images:listImageTags | Querying project tags     | list         | -                           | -                                                                                                              | -               |

An IMS API usually supports one or more actions. [Table 3-14](#) lists the supported actions and dependencies.

**Table 3-14** Actions and dependencies supported by IMS APIs

| API                                                                     | Action                     | Dependencies                                                                                         |
|-------------------------------------------------------------------------|----------------------------|------------------------------------------------------------------------------------------------------|
| GET /v2/cloudimages                                                     | ims:images:list            | -                                                                                                    |
| GET /v2/images/{image_id}                                               | ims:images:get             | -                                                                                                    |
| POST /v2/images                                                         | ims:images:create          | -                                                                                                    |
| POST /v2/images/{image_id}/members                                      | ims:images:share           | ims:images:get                                                                                       |
| POST /v1/cloudimages/{image_id}/copy                                    | ims:images:copyInRegion    | ims:serverImages:create                                                                              |
| POST /v1/cloudimages/{image_id}/cross_region_copy                       | ims:images:copyCrossRegion | -                                                                                                    |
| GET /v1/cloudimages/quota                                               | ims:quotas:get             | -                                                                                                    |
| PUT /v1/cloudimages/{image_id}/upload<br>PUT /v2/images/{image_id}/file | ims:images:upload          | <ul style="list-style-type: none"> <li>ims:images:get</li> <li>ims:images:update</li> </ul>          |
| POST /v1/cloudimages/wholeimages/action                                 | ims:wholeImages:create     | -                                                                                                    |
| POST /v1/cloudimages/{image_id}/file                                    | ims:images:export          | <ul style="list-style-type: none"> <li>obs:object:GetObject</li> <li>obs:object:PutObject</li> </ul> |

| API                                                                                                                                                                                                                                                                                                                                                                          | Action                     | Dependencies                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>POST /v2/cloudimages/quickimport/action (required only for quickly importing a data disk image)</li> <li>POST /v1/cloudimages/dataimages/action</li> </ul>                                                                                                                                                                            | ims:dataImages:create      | -                                                                                                        |
| <ul style="list-style-type: none"> <li>PATCH /v2/cloudimages/{image_id} (required only for enterprise project migration)</li> <li>POST /v2/cloudimages/action</li> <li>OST /v2/cloudimages/quickimport/action (required only for quickly importing a system disk image)</li> <li>POST /v1/cloudimages/{image_id}/copy (required only by enterprise project users)</li> </ul> | ims:serverImages:create    | -                                                                                                        |
| PUT /v1/cloudimages/tags                                                                                                                                                                                                                                                                                                                                                     | ims:images:setTags         | -                                                                                                        |
| GET /v1/cloudimages/tags                                                                                                                                                                                                                                                                                                                                                     | ims:images:getTags         | -                                                                                                        |
| DELETE /v2/images/{image_id}                                                                                                                                                                                                                                                                                                                                                 | ims:images:deleteImage     | -                                                                                                        |
| <ul style="list-style-type: none"> <li>PATCH /v2/cloudimages/{image_id}</li> <li>PATCH /v2/images/{image_id}</li> </ul>                                                                                                                                                                                                                                                      | ims:images:updateImage     | -                                                                                                        |
| GET /v1/cloudimages/os_version                                                                                                                                                                                                                                                                                                                                               | ims:images:listOsVersion   | -                                                                                                        |
| GET /v1/cloudimages/job/{job_id}                                                                                                                                                                                                                                                                                                                                             | ims:images:getJob          | -                                                                                                        |
| POST /v2/cloudimages/quickimport/action                                                                                                                                                                                                                                                                                                                                      | ims:images:import          | <ul style="list-style-type: none"> <li>ims:dataImages:create</li> <li>ims:serverImages:create</li> </ul> |
| POST /v2/{project_id}/images/{image_id}/tags/action                                                                                                                                                                                                                                                                                                                          | ims:images:setOrDeleteTags | <ul style="list-style-type: none"> <li>ims:images:setTags</li> <li>ims:images:deleteTags</li> </ul>      |

| API                                                                                                                                  | Action                        | Dependencies |
|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|--------------|
| <ul style="list-style-type: none"> <li>PUT /v1/cloudimages/members</li> <li>PUT /v2/images/{image_id}/members/{member_id}</li> </ul> | ims:images:updateMemberStatus | -            |
| POST /v1/cloudimages/members                                                                                                         | ims:images:addMember          | -            |
| DELETE /v1/cloudimages/members                                                                                                       | ims:images:deleteMember       | -            |
| POST /v2/{project_id}/images/resource_instances/action                                                                               | ims:images:listImagesByTag    | -            |
| GET /v2/{project_id}/images/{image_id}/tags                                                                                          | ims:images:showImageTags      | -            |
| GET /v2/{project_id}/images/tags                                                                                                     | ims:images:listImageTags      | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-15](#), a resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can specify in identity policy statements for IMS.

**Table 3-15** Resource types supported by IMS

| Resource Type | URN                                        |
|---------------|--------------------------------------------|
| Image         | ims:<region>:<account-id>:image:<image-id> |

- <region> indicates the region where a user is authorized to perform operations.
- <account-id> indicates the ID of an authorized user account. Obtain an account ID as instructed in [API Credentials](#).
- <image-id> indicates the ID of the image on which a user is authorized to perform operations.

 **NOTE**

You can use a wildcard (\*) in URN to indicate all resources.

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global or service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, IAM automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **ims:**) only apply to operations of IMS. For details, see [Table 3-16](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

The following table lists the condition keys that you can define in identity policies for IMS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-16** Service-specific condition keys supported by IMS

| Condition Key      | Value Type | Single-valued/<br>Multivalued | Description                                                                                     |
|--------------------|------------|-------------------------------|-------------------------------------------------------------------------------------------------|
| ims:TargetOrgPaths | string     | Multivalued                   | Filters access based on the <b>Organizations Path</b> of the specified sharing account.         |
| ims:Encrypted      | boolean    | Single-valued                 | Controls operations such as image import and replication based on whether images are encrypted. |

| Condition Key              | Value Type | Single-valued/<br>Multivalued | Description                                                                                              |
|----------------------------|------------|-------------------------------|----------------------------------------------------------------------------------------------------------|
| ims:TargetBucketOrgPaths   | string     | Multivalued                   | Filters access based on the <b>Organizations Path</b> of the specified destination bucket owner account. |
| ims:OriginBucketOrgPaths   | string     | Multivalued                   | Filters access based on the <b>Organizations Path</b> of the specified source bucket owner account.      |
| ims:SourceAvailabilityZone | string     | Multivalued                   | Filters access based on the specified AZ.                                                                |
| ims:InstanceId             | string     | Single-valued                 | Controls full-ECS image creation based on the specified ECS ID.                                          |
| ims:VaultId                | string     | Single-valued                 | Controls creation and cross-region replication of full-ECS images based on the specified vault ID.       |
| ims:VolumeId               | string     | Multivalued                   | Controls image creation based on the specified volume ID.                                                |
| ims:BackupId               | string     | Single-valued                 | Controls full-ECS image creation based on the specified backup ID.                                       |
| ims:Region                 | string     | Single-valued                 | Controls cross-region replication based on the specified destination region.                             |

### 3.1.5 FunctionGraph

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service provides **Service Control Policies (SCPs)** to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the defined resource types, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the defined condition keys, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for FunctionGraph.



**Table 3-17** Supported Actions

| Action                                 | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                            |
|----------------------------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| functiongraph:function:createFunction  | Grants permission to create a function.            | Write        | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • functiongraph:function:create  |
|                                        |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                  |
| functiongraph:function:deleteFunction  | Grants permission to delete a function.            | Write        | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • functiongraph:function:delete  |
|                                        |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                  |
| functiongraph:function:listFunctions   | Grants permission to list functions.               | List         | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • functiongraph:function:list    |
|                                        |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                  |
| functiongraph:function:getFunctionCode | Grants permission to query the code of a function. | Read         | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • functiongraph:function:getCode |

| Action                                      | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                               |
|---------------------------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
|                                             |                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                     |
| functiongraph:function:updateFunctionCode   | Grants permission to modify the code of a function.     | Write        | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | functiongraph:function:updateCode   |
|                                             |                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                     |
| functiongraph:function:getFunctionConfig    | Grants permission to query the metadata of a function.  | Read         | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | functiongraph:function:getConfig    |
|                                             |                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                     |
| functiongraph:function:updateFunctionConfig | Grants permission to modify the metadata of a function. | Write        | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | functiongraph:function:updateConfig |
|                                             |                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                     |

| Action                                         | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                 |
|------------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| functiongraph:function:updateMaxInstanceConfig | Grants permission to update the maximum number of instances of a function. | Write        | function *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • functiongraph:function:updateConfig |
|                                                |                                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                       |
| functiongraph:function:updateSnapshot          | Grants permission to enable or disable snapshot for a function.            | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | • functiongraph:function:updateConfig |
| functiongraph:function:getSnapshotState        | Grants permission to query the snapshot status of a function.              | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | • functiongraph:function:updateConfig |
| functiongraph:function:createUrl               | Grants permission to create a function URL.                                | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | • functiongraph:function:updateConfig |
| functiongraph:function:deleteUrl               | Grants permission to delete a function URL.                                | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | • functiongraph:function:updateConfig |
| functiongraph:function:updateUrl               | Grants permission to update a function URL.                                | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | • functiongraph:function:updateConfig |
| functiongraph:function:getUrl                  | Grants permission to query the URL of a function.                          | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | • functiongraph:function:updateConfig |

| Action                             | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                    | Alias                                                                                 |
|------------------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| functiongraph::getResourceInstance | Grants permission to query resources.                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | <ul style="list-style-type: none"> <li>functiongraph:function:updateConfig</li> </ul> |
| functiongraph::createTag           | Grants permission to create resource tags.               | Tagging      | -                           | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>functiongraph:function:updateConfig</li> </ul> |
| functiongraph::deleteTag           | Grants permission to delete resource tags.               | Tagging      | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | <ul style="list-style-type: none"> <li>functiongraph:function:updateConfig</li> </ul> |
| functiongraph::listTags            | Grants permission to list resource tags.                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | <ul style="list-style-type: none"> <li>functiongraph:function:updateConfig</li> </ul> |
| functiongraph::createFunctionApp   | Grants permission to create an application.              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>         |
| functiongraph::deleteFunctionApp   | Grants permission to delete an application.              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | <ul style="list-style-type: none"> <li>functiongraph:function:delete</li> </ul>       |
| functiongraph::getFunctionApp      | Grants permission to query details about an application. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>         |
| functiongraph::listFunctionApps    | Grants permission to list applications.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>         |

| Action                                  | Description                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                                 |
|-----------------------------------------|-----------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------------------|
| functiongraph::listFunctionAppTemplates | Grants permission to list application templates.    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>         |
| functiongraph::createVpcEndpoint        | Grants permission to create a VPC endpoint.         | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:updateConfig</li> </ul> |
| functiongraph::deleteVpcEndpoint        | Grants permission to delete a VPC endpoint.         | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:delete</li> </ul>       |
| functiongraph::function:export          | Grants permission to export a function.             | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul>    |
| functiongraph::function:import          | Grants permission to import a function.             | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>       |
| functiongraph::exportPackage            | Grants permission to export a function application. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>         |
| functiongraph::importPackage            | Grants permission to import a function application. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>       |
| functiongraph::function:createVersion   | Grants permission to publish a function version.    | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                                     |

| Action                             | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                         |
|------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------------------|
| functiongraph:function:listVersion | Grants permission to list the versions of a function.                     | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                             |
| functiongraph:function:createAlias | Grants permission to create an alias for a function's additional version. | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                             |
| functiongraph:function:deleteAlias | Grants permission to delete an alias of a function version.               | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                             |
| functiongraph:function:listAliases | Grants permission to list the versions and aliases of a function.         | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                             |
| functiongraph:function:getAlias    | Grants permission to query an alias of a function version.                | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                             |
| functiongraph:function:updateAlias | Grants permission to modify an alias of a function version.               | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                             |
| functiongraph::listQuota           | Grants permission to query tenant quotas.                                 | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul> |

| Action                                           | Description                                             | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                               |
|--------------------------------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------------------------------------------------------|
| functiongraph:dependency:createDependency        | Grants permission to create a dependency.               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>     |
| functiongraph:dependency:deleteDependency        | Grants permission to delete a dependency.               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:delete</li> </ul>     |
| functiongraph:dependency:listDependencies        | Grants permission to list the dependencies.             | List         | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>       |
| functiongraph:dependency:getDependency           | Grants permission to query a dependency.                | Read         | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:getcode</li> </ul>    |
| functiongraph:dependency:updateDependency        | Grants permission to update a dependency.               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:updatecode</li> </ul> |
| functiongraph:dependency:createDependencyVersion | Grants permission to create a dependency version.       | Write        | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>     |
| functiongraph:dependency:deleteDependencyVersion | Grants permission to delete a dependency version.       | Write        | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:delete</li> </ul>     |
| functiongraph:dependency:listDependencyVersion   | Grants permission to list the versions of a dependency. | List         | -                           | -             | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>       |

| Action                                        | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                            |
|-----------------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------------------|
| functiongraph:dependency:getDependencyVersion | Grants permission to query details about a dependency version.        | Read         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:getcode</li> </ul> |
| functiongraph:function:createEvent            | Grants permission to create a test event.                             | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>  |
| functiongraph:function:deleteEvent            | Grants permission to delete a test event.                             | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>  |
| functiongraph:function:updateEvent            | Grants permission to update a test event.                             | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>  |
| functiongraph:function:listEvent              | Grants permission to list the test events of a function.              | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>    |
| functiongraph:function:getEvent               | Grants permission to query details about a test event of a function.  | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>  |
| functiongraph:function:getTracing             | Grants permission to query the tracing configurations of a function.  | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>  |
| functiongraph:function:updateTracing          | Grants permission to update the tracing configurations of a function. | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>  |



| Action                                             | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                              |
|----------------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------------|
| functiongraph::listFunctionByMetric                | Grants permission to query functions for a specified metric.                    | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>      |
| functiongraph::function:listFunctionStatistics     | Grants permission to query metrics of a function in a specified period.         | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul> |
| functiongraph::listStatistics                      | Grants permission to query function statistics.                                 | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul> |
| functiongraph::function:getReservedInstanceMetrics | Grants permission to query the reserved instance usage of a function.           | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul> |
| functiongraph::enableLtsLogs                       | Grants permission to enable log reporting to LTS.                               | Write        | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>    |
| functiongraph::function:getLtsLogConfiguration     | Grants permission to query the LTS log group and stream settings of a function. | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul> |

| Action                                              | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                                 |
|-----------------------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------------------|
| functiongraph::function:updateReservedInstanceCount | Grants permission to change the number of reserved instances of a function.    | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:updateconfig</li> </ul> |
| functiongraph::listReservedInstanceCount            | Grants permission to query the number of reserved instances of a function.     | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul>    |
| functiongraph::listReservedInstanceConfig           | Grants permission to query the reserved instance configurations of a function. | List         | function                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul>    |
| functiongraph::getReservedInstanceState             | Grants permission to query the status of reserved instances of a function.     | Read         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul>    |
| functiongraph::function:invokeAsync                 | Grants permission to execute a function asynchronously.                        | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                                     |
| functiongraph::function:invokeSync                  | Grants permission to execute a function synchronously.                         | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>       |

| Action                                             | Description                                                                              | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                                 |
|----------------------------------------------------|------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------------------|
| functiongraph:function:invokeReservedFunctionAsync | Grants permission to execute a function asynchronously and return reserved instance IDs. | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invokeasync</li> </ul>  |
| functiongraph:function:stopAsyncInvoke             | Grants permission to stop an asynchronous invocation request of a function.              | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invokeasync</li> </ul>  |
| functiongraph:function:listAsyncInvocations        | Grants permission to query asynchronous invocation requests of a function.               | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>         |
| functiongraph:function:deleteAsyncInvokeConfig     | Grants permission to delete the asynchronous invocation settings of a function.          | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:delete</li> </ul>       |
| functiongraph:function:updateAsyncInvokeConfig     | Grants permission to configure asynchronous invocation settings for a function.          | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:updateconfig</li> </ul> |

| Action                                            | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                              |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------------|
| functiongraph:function:listAsyncInvokeConfig      | Grants permission to query the asynchronous invocation settings of a function's all versions. | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>      |
| functiongraph:function:getAsyncInvokeConfig       | Grants permission to query the asynchronous invocation setting of a function version.         | Read         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getconfig</li> </ul> |
| functiongraph::updateAsyncStatusLog               | Grants permission to enable asynchronous notification.                                        | Write        | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>    |
| functiongraph::getAsyncStatusLogInfo              | Grants permission to query details about asynchronous invocation logs.                        | Read         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:getConfig</li> </ul> |
| functiongraph:function:listActiveAsyncInvocations | Grants permission to query active asynchronous invocation requests of a function.             | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>      |
| functiongraph:trigger:createTrigger               | Grants permission to create a trigger.                                                        | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:trigger:create</li> </ul>     |

| Action                              | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                                                   |
|-------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------|
| functiongraph:trigger:delete        | Grants permission to delete a trigger.                                 | Write        | trigger *                   | <a href="#">g:EnterpriseProjectId</a> | -                                                                                                       |
| functiongraph:trigger:update        | Grants permission to update a trigger.                                 | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:trigger:create</li> </ul>                          |
| functiongraph:trigger:list          | Grants permission to list all triggers of a function.                  | List         | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:trigger:listSpecifiedFunctionTriggers</li> </ul>   |
| functiongraph:trigger:get           | Grants permission to query a trigger.                                  | Read         | trigger *                   | <a href="#">g:EnterpriseProjectId</a> | -                                                                                                       |
| functiongraph:trigger:batch Delete  | Grants permission to delete all triggers of a function.                | Write        | function *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:trigger:deleteSpecifiedFunctionTriggers</li> </ul> |
| functiongraph::listObsNotifications | Grants permission to query all notification settings of an OBS bucket. | Read         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:trigger:create</li> </ul>                          |
| functiongraph::listObsBucket        | Grants permission to list the OBS buckets.                             | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:trigger:listSpecifiedFunctionTriggers</li> </ul>   |
| functiongraph:workflow:create       | Grants permission to create a function flow.                           | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>                         |

| Action                            | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                              |
|-----------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------------|
| functiongraph:workflow:delete     | Grants permission to delete a function flow.                          | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:delete</li> </ul>    |
| functiongraph:workflow:update     | Grants permission to modify the instance metadata of a function flow. | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:create</li> </ul>    |
| functiongraph:workflow:list       | Grants permission to query a function flow.                           | List         | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>      |
| functiongraph:workflow:getConfig  | Grants permission to query the instance metadata of a function flow.  | Read         | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getConfig</li> </ul> |
| functiongraph:workflow:invoke     | Grants permission to execute a function flow asynchronously.          | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>    |
| functiongraph:workflow:invokeSync | Grants permission to execute a function flow synchronously.           | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>    |
| functiongraph:workflow:terminate  | Grants permission to stop a function flow.                            | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>    |
| functiongraph:workflow:retry      | Grants permission to retry a function flow.                           | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>    |

| Action                                     | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                              |
|--------------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------------|
| functiongraph:workflow:list Executions     | Grants permission to list the instances of a function flow.                  | List         | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>      |
| functiongraph:workflow:get ExecutionDetail | Grants permission to query a function flow instance.                         | Read         | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getConfig</li> </ul> |
| functiongraph:workflow:get Metric          | Grants permission to query the metrics of a function flow.                   | Read         | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getConfig</li> </ul> |
| functiongraph:workflow:list Metrics        | Grants permission to query function flow metrics.                            | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:getConfig</li> </ul> |
| functiongraph:workflow:downloadOutput      | Grants permission to download the node execution results of a function flow. | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:getConfig</li> </ul> |
| functiongraph:workflow:cancel              | Grants permission to stop executing a function flow.                         | Write        | workflow *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>functiongraph:function:invoke</li> </ul>    |
| functiongraph:workflow:metadata            | Grants permission to query the metadata of a function flow.                  | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>functiongraph:function:list</li> </ul>      |

Each API usually supports one or more actions. [Table 3-18](#) lists the supported actions and dependencies.

**Table 3-18** Actions and dependencies supported by FunctionGraph APIs

| API                                                      | Action                                      | Dependency                                                                                                                                                                                         |
|----------------------------------------------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/fgs/functions                      | functiongraph:function:createFunction       | <ul style="list-style-type: none"> <li>• lts:groups:list</li> <li>• lts:groups:create</li> <li>• lts:logstreams:list</li> <li>• lts:structConfig:create</li> <li>• obs:object:GetObject</li> </ul> |
| DELETE /v2/{project_id}/fgs/functions/{function_urn}     | functiongraph:function:deleteFunction       | <ul style="list-style-type: none"> <li>• functiongraph:trigger:batchDelete</li> <li>• lts:groups:list</li> <li>• lts:logstreams:list</li> <li>• lts:logstreams:delete</li> </ul>                   |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/config | functiongraph:function:updateFunctionConfig | <ul style="list-style-type: none"> <li>• lts:groups:list</li> <li>• lts:groups:create</li> <li>• lts:logstreams:list</li> <li>• lts:structConfig:create</li> </ul>                                 |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/code   | functiongraph:function:updateFunctionCode   | obs:object:GetObject                                                                                                                                                                               |
| GET /v2/{project_id}/fgs/functions                       | functiongraph:function:listFunctions        | -                                                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/functions/{function_urn}/config | functiongraph:function:getFunctionConfig    | -                                                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/functions/{function_urn}/code   | functiongraph:function:getFunctionCode      | -                                                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/public-network-bandwidth        | functiongraph::getPublicNetworkBandwidth    | -                                                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/resource-usage                  | functiongraph::getTenantResourceUsage       | -                                                                                                                                                                                                  |



| API                                                                   | Action                                         | Dependency |
|-----------------------------------------------------------------------|------------------------------------------------|------------|
| POST /v2/{project_id}/fgs/functions/{function_urn}/command            | functiongraph::function:createTenantCommand    | -          |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/config-max-instance | functiongraph:function:updateMaxInstanceConfig | -          |
| POST /v2/{project_id}/fgs/functions/{function_urn}/snapshots/{action} | functiongraph:function:updateSnapshot          | -          |
| POST /v2/{project_id}/fgs/functions/{function_urn}/function-url       | functiongraph:function:createUrl               | -          |
| DELETE /v2/{project_id}/fgs/functions/{function_urn}/function-url     | functiongraph:function:deleteUrl               | -          |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/function-url        | functiongraph:function:updateUrl               | -          |
| GET /v2/{project_id}/fgs/functions/{function_urn}/function-url        | functiongraph:function:getUrl                  | -          |
| POST /v2/{project_id}/{resource_type}/resource-instances/{action}     | functiongraph::getResourceInstance             | -          |
| POST /v2/{project_id}/{resource_type}/{resource_id}/tags/create       | functiongraph::createTag                       | -          |

| API                                                               | Action                                     | Dependency |
|-------------------------------------------------------------------|--------------------------------------------|------------|
| DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/delete | functiongraph::deleteTag                   | -          |
| GET /v2/{project_id}/{resource_type}/tags                         | functiongraph::listTags                    | -          |
| POST /v2/{project_id}/fgs/applications                            | functiongraph::createFunctionApp           | -          |
| DELETE /v2/{project_id}/fgs/applications/{id}                     | functiongraph::deleteFunctionApp           | -          |
| GET /v2/{project_id}/fgs/applications/{id}                        | functiongraph::getFunctionApp              | -          |
| GET /v2/{project_id}/fgs/applications                             | functiongraph::listFunctionApps            | -          |
| GET /v2/{project_id}/fgs/application/templates                    | functiongraph::listFunctionAppTemplates    | -          |
| POST /v2/{project_id}/fgs/vpc-endpoint                            | functiongraph::createVpcEndpoint           | -          |
| DELETE /v2/{project_id}/fgs/vpc-endpoint/{vpc_id}/{subnet_id}     | functiongraph::deleteVpcEndpoint           | -          |
| GET /v2/{project_id}/fgs/functions/{func_urn}/download            | functiongraph::function::getFunctionCode   | -          |
| GET /v2/{project_id}/fgs/admins/sysconfig                         | functiongraph::function::getFunctionConfig | -          |

| API                                                                      | Action                                      | Dependency    |
|--------------------------------------------------------------------------|---------------------------------------------|---------------|
| GET /v2/{project_id}/fgs/domainname/vpc/{vpc_id}                         | functiongraph:function:getFunctionConfig    | dns:zone:list |
| GET /v2/{project_id}/fgs/functions/{function_urn}/servicebridge/relation | functiongraph:function:listFunctions        | -             |
| POST /v2/{project_id}/fgs/packages                                       | functiongraph:function:createFunction       | -             |
| DELETE /v2/{project_id}/fgs/packages/{package_name}                      | functiongraph:function:deleteFunction       | -             |
| PUT /v2/{project_id}/fgs/packages/{package_name}                         | functiongraph:function:createFunction       | -             |
| GET /v2/{project_id}/fgs/packages                                        | functiongraph:function:listFunctions        | -             |
| PUT /v2/{project_id}/fgs/functions/{func_urn}/collect/{state}            | functiongraph:function:updateFunctionConfig | -             |
| GET /v2/{project_id}/fgs/template-labels                                 | functiongraph:function:listFunctions        | -             |
| GET /v2/fgs/template-labels                                              | functiongraph:function:listFunctions        | -             |
| GET /v2/{project_id}/fgs/templates                                       | functiongraph:function:listFunctions        | -             |
| GET /v2/{project_id}/fgs/templates/{template_id}                         | functiongraph:function:listFunctions        | -             |
| GET /v2/fgs/runtimetypes                                                 | functiongraph:function:listFunctions        | -             |

| API                                                                        | Action                                            | Dependency                                                                                                                                                         |
|----------------------------------------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v2/fgs/service-trusted-agencies                                       | functiongraph:function:getFunctionConfig          | -                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/feature                                           | functiongraph:function:getFunctionConfig          | -                                                                                                                                                                  |
| POST /v2/{project_id}/fgs/agc/agency/{agency_name}                         | functiongraph:function:createFunction             | -                                                                                                                                                                  |
| POST /v2/{project_id}/fgs/functions/enable-async-status-logs               | functiongraph::updateAsyncStatusLog               | <ul style="list-style-type: none"> <li>• lts:groups:list</li> <li>• lts:groups:create</li> <li>• lts:logstreams:list</li> <li>• lts:structConfig:create</li> </ul> |
| GET /v2/{project_id}/fgs/functions/async-status-log-detail                 | functiongraph::getAsyncStatusLogInfo              | -                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/functions/{function_urn}/active-async-invocations | functiongraph:function:listActiveAsyncInvocations | -                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/functions/{function_urn}/export                   | functiongraph:function:export                     | -                                                                                                                                                                  |
| POST /v2/{project_id}/fgs/functions/import                                 | functiongraph:function:import                     | -                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/packages/{package_name}/export                    | functiongraph::exportPackage                      | -                                                                                                                                                                  |
| POST /v2/{project_id}/fgs/packages/import                                  | functiongraph::importPackage                      | -                                                                                                                                                                  |

| API                                                                       | Action                                    | Dependency                 |
|---------------------------------------------------------------------------|-------------------------------------------|----------------------------|
| POST /v2/{project_id}/fgs/functions/{function_urn}/versions               | functiongraph:function:createVersion      | -                          |
| GET /v2/{project_id}/fgs/functions/{function_urn}/versions                | functiongraph:function:listVersion        | -                          |
| POST /v2/{project_id}/fgs/functions/{function_urn}/aliases                | functiongraph:function:createAlias        | -                          |
| DELETE /v2/{project_id}/fgs/functions/{function_urn}/aliases/{alias_name} | functiongraph:function:deleteAlias        | functiongraph:trigger:list |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/aliases/{alias_name}    | functiongraph:function:updateAlias        | -                          |
| GET /v2/{project_id}/fgs/functions/{function_urn}/aliases                 | functiongraph:function:listAlias          | -                          |
| GET /v2/{project_id}/fgs/functions/{function_urn}/aliases/{alias_name}    | functiongraph:function:getAlias           | -                          |
| POST /v2/{project_id}/fgs/dependencies                                    | functiongraph:dependency:createDependency | obs:object:GetObject       |
| DELETE /v2/{project_id}/fgs/dependencies/{depend_id}                      | functiongraph:dependency:deleteDependency | -                          |

| API                                                                    | Action                                           | Dependency           |
|------------------------------------------------------------------------|--------------------------------------------------|----------------------|
| PUT /v2/{project_id}/fgs/dependencies/{depend_id}                      | functiongraph:dependency:updateDependency        | obs:object:GetObject |
| GET /v2/{project_id}/fgs/dependencies                                  | functiongraph:dependency:listDependencies        | -                    |
| GET /v2/{project_id}/fgs/dependencies/{depend_id}                      | functiongraph:dependency:getDependency           | -                    |
| POST /v2/{project_id}/fgs/dependencies/version                         | functiongraph:dependency:createDependencyVersion | obs:object:GetObject |
| DELETE /v2/{project_id}/fgs/dependencies/{depend_id}/version/{version} | functiongraph:dependency:deleteDependencyVersion | -                    |
| GET /v2/{project_id}/fgs/dependencies/{depend_id}/version              | functiongraph:dependency:listDependencyVersion   | -                    |
| GET /v2/{project_id}/fgs/dependencies/{depend_id}/version/{version}    | functiongraph:dependency:getDependencyVersion    | -                    |
| POST /v2/{project_id}/fgs/functions/{function_urn}/events              | functiongraph:function:createEvent               | -                    |
| DELETE /v2/{project_id}/fgs/functions/{function_urn}/events/{event_id} | functiongraph:function:deleteEvent               | -                    |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/events/{event_id}    | functiongraph:function:updateEvent               | -                    |

| API                                                                 | Action                                             | Dependency                                                                                                                                                         |
|---------------------------------------------------------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v2/{project_id}/fgs/functions/{function_urn}/events            | functiongraph:function:listEvent                   | -                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/functions/{function_urn}/events/{event_id} | functiongraph:function:getEvent                    | -                                                                                                                                                                  |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/tracing           | functiongraph:function:updateTracing               | -                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/functions/{function_urn}/tracing           | functiongraph:function:getTracing                  | -                                                                                                                                                                  |
| GET /v2/{project_id}/fgs/function/report                            | functiongraph::listFunctionByMetric                | <ul style="list-style-type: none"> <li>• aom:metric:get</li> <li>• aom:metric:list</li> </ul>                                                                      |
| GET /v2/{project_id}/fgs/functions/statistics                       | functiongraph::listStatistics                      | aom:metric:get                                                                                                                                                     |
| POST /v2/{project_id}/fgs/functions/enable-lts-logs                 | functiongraph::enableLtsLogs                       | <ul style="list-style-type: none"> <li>• lts:groups:list</li> <li>• lts:groups:create</li> <li>• lts:logstreams:list</li> <li>• lts:structConfig:create</li> </ul> |
| GET /v2/{project_id}/fgs/functions/{function_urn}/lts-log-detail    | functiongraph:function:getLtsLogConfiguration      | -                                                                                                                                                                  |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/reservedinstances | functiongraph:function:updateReservedInstanceCount | -                                                                                                                                                                  |

| API                                                                      | Action                                         | Dependency                                                                                                    |
|--------------------------------------------------------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| GET /v2/{project_id}/fgs/functions/reservedinstances                     | functiongraph::listReservedInstanceCount       | -                                                                                                             |
| GET /v2/{project_id}/fgs/functions/reservedinstance-configs              | functiongraph::listReservedInstanceConfig      | -                                                                                                             |
| GET /v2/{project_id}/fgs/functions/reservedinstances/state               | functiongraph::getReservedInstanceState        | -                                                                                                             |
| POST /v2/{project_id}/fgs/functions/{function_urn}/cancel                | functiongraph:function:stopAsyncInvoke         | lts:structConfig:get                                                                                          |
| GET /v2/{project_id}/fgs/functions/{function_urn}/async-invocations      | functiongraph:function:listAsyncInvocation     | <ul style="list-style-type: none"> <li>lts:structConfig:get</li> <li>lts:logStream:searchStructLog</li> </ul> |
| DELETE /v2/{project_id}/fgs/functions/{function_urn}/async-invoke-config | functiongraph:function:deleteAsyncInvokeConfig | -                                                                                                             |
| PUT /v2/{project_id}/fgs/functions/{function_urn}/async-invoke-config    | functiongraph:function:updateAsyncInvokeConfig | -                                                                                                             |
| GET /v2/{project_id}/fgs/functions/{function_urn}/async-invoke-configs   | functiongraph:function:listAsyncInvokeConfig   | -                                                                                                             |
| GET /v2/{project_id}/fgs/functions/{function_urn}/async-invoke-config    | functiongraph:function:getAsyncInvokeConfig    | -                                                                                                             |



| API                                                         | Action                                         | Dependency |
|-------------------------------------------------------------|------------------------------------------------|------------|
| POST /v2/{project_id}/fgs/servicebridge                     | functiongraph:bridge:createServiceBridge       | -          |
| DELETE /v2/{project_id}/fgs/servicebridge/{bridge_name}     | functiongraph:bridge:deleteServiceBridge       | -          |
| PUT /v2/{project_id}/fgs/servicebridge/{bridge_name}/config | functiongraph:bridge:updateServiceBridgeConfig | -          |
| GET /v2/{project_id}/fgs/servicebridge                      | functiongraph:bridge:listServiceBridges        | -          |
| GET /v2/{project_id}/fgs/servicebridge/{bridge_name}/config | functiongraph:bridge:getServiceBridgeConfig    | -          |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-19](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for FunctionGraph.

**Table 3-19** Supported resource types

| Resource Type | URN                                                                         |
|---------------|-----------------------------------------------------------------------------|
| workflow      | functiongraph:<region>:<account-id>:workflow:<workflow-id>                  |
| function      | functiongraph:<region>:<account-id>:function:<package-name>/<function-name> |
| trigger       | functiongraph:<region>:<account-id>:trigger:<trigger-id>                    |

## Conditions

FunctionGraph does not support service-specific condition keys in policies.

It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.1.6 Cloud Data Center

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include [actions](#), [resources](#), and [conditions](#).

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (such as **List**, **Read**, **Write**, or **Tagging**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources (\*) in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CloudDC, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CloudDC, see [Conditions](#).

The following table lists the actions that you can define in identity policy statements for CloudDC.

**Table 3-20** Actions supported by CloudDC

| Action                              | Description                                      | Access Level | Resource Condition Key                         | Global Condition Key |
|-------------------------------------|--------------------------------------------------|--------------|------------------------------------------------|----------------------|
| clouddc:imetal:list                 | Batch querying physical servers                  | list         | -                                              | -                    |
| clouddc:imetal:get                  | Querying information about physical servers      | read         | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |
| clouddc:imetal:getHardwareAttribute | Querying server hardware details                 | read         | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |
| clouddc:imetal:getFirmwareAttribute | Querying server firmware details                 | read         | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |
| clouddc:imetal:updatePowerStatus    | Modifying the power statuses of physical servers | write        | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |
| clouddc:imetal:createDumpLog        | Exporting server logs                            | write        | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |
| clouddc:imetal:getDumpLogProgress   | Querying the export status of logs               | read         | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |

| Action                                 | Description                            | Access Level | Resource Condition Key                         | Global Condition Key |
|----------------------------------------|----------------------------------------|--------------|------------------------------------------------|----------------------|
| cloudcc:imetal:createDownloadLog       | Downloading logs                       | write        | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |
| cloudcc:imetal:createRemoteConsoleLink | Obtaining the console address          | write        | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |
| cloudcc:instance:createBatch           | Batch creating instances               | write        | -                                              | -                    |
| cloudcc:instance:list                  | Batch querying instances               | list         | -                                              | -                    |
| cloudcc:instance:deleteBatch           | Batch deleting instances               | write        | -                                              | -                    |
| cloudcc:instance:create                | Creating an instance                   | write        | -                                              | -                    |
| cloudcc:instance:delete                | Deleting an instance                   | write        | -                                              | -                    |
| cloudcc:instance:changePassword        | Changing the password of an instance   | write        | -                                              | -                    |
| cloudcc:instance:reinstallOS           | Reinstalling the OS on an instance     | write        | -                                              | -                    |
| cloudcc:instance:get                   | Querying the status of an instance     | read         | -                                              | -                    |
| cloudcc:instance:updateIP              | Changing the IP address of an instance | write        | -                                              | -                    |
| cloudcc::listResourcesByTag            | Listing resources                      | list         | -                                              | g:TagKeys            |
| cloudcc::listTagsForResource           | Querying tags of a resource            | list         | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                    |

| Action                      | Description                                    | Access Level | Resource Condition Key                         | Global Condition Key                |
|-----------------------------|------------------------------------------------|--------------|------------------------------------------------|-------------------------------------|
| cloudcc::listTags           | Querying resource tags in a specified project. | list         | -                                              | -                                   |
| cloudcc::listResourcesByTag | Querying the number of instances               | list         | -                                              | g:TagKeys                           |
| cloudcc::tagResource        | Batch creating iMetal server tags              | tagging      | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | g:RequestTag/<tag-key><br>g:TagKeys |
| cloudcc::unTagResource      | Batch deleting iMetal server tags              | tagging      | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | g:RequestTag/<tag-key><br>g:TagKeys |
| cloudcc::listStatus         | Obtaining server overview                      | list         | -                                              | -                                   |
| cloudcc::listAlarmStat      | Obtaining server alarm overview                | list         | -                                              | -                                   |
| cloudcc::listAlarmTrend     | Obtaining the server alarm trend               | list         | -                                              | -                                   |
| cloudcc::listAlarm          | Obtaining the server alarm list                | list         | -                                              | -                                   |
| cloudcc::listEvent          | Obtaining the server event list                | list         | -                                              | -                                   |
| cloudcc::listEventDicts     | Querying event definitions                     | list         | -                                              | -                                   |
| cloudcc::updateRepairs      | Updating or creating server maintenance data   | write        | -                                              | -                                   |

| Action                       | Description                                | Access Level | Resource Condition Key                         | Global Condition Key                 |
|------------------------------|--------------------------------------------|--------------|------------------------------------------------|--------------------------------------|
| cloudcc::listRepairs         | Querying server maintenance data           | list         | -                                              | -                                    |
| cloudcc::updateSpareParts    | Creating and updating spare parts          | write        | -                                              | -                                    |
| cloudcc::listSpareParts      | Querying spare parts                       | list         | -                                              | -                                    |
| cloudcc:irack:update         | Modifying the intelligent rack description | write        | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                                    |
| cloudcc:irack:list           | Querying the intelligent rack list         | list         | -                                              | -                                    |
| cloudcc:idc:update           | Modifying the IDC description              | write        | -                                              | -                                    |
| cloudcc:idc:list             | Querying the IDC list                      | list         | -                                              | -                                    |
| cloudcc::listResourcesByTag  | Querying the rack list                     | list         | -                                              | g:TagKeys                            |
| cloudcc::listTagsForResource | Querying rack tags                         | list         | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | -                                    |
| cloudcc::listTags            | Querying rack tags in a specified project  | list         | -                                              | -                                    |
| cloudcc::listResourcesByTag  | Querying the number of racks               | list         | -                                              | g:TagKeys                            |
| cloudcc::tagResource         | Batch creating rack tags                   | tagging      | <a href="#">g:ResourceTag /&lt;tag-key&gt;</a> | g:RequestTag /<tag-key><br>g:TagKeys |

| Action                   | Description                                    | Access Level | Resource Condition Key                        | Global Condition Key                |
|--------------------------|------------------------------------------------|--------------|-----------------------------------------------|-------------------------------------|
| clouddc::unTagResource   | Batch deleting rack tags                       | tagging      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | g:RequestTag/<tag-key><br>g:TagKeys |
| clouddc::createRackOrder | Granting permissions to check order parameters | write        | -                                             | -                                   |

Each API of CloudDC usually supports one or more actions. [Table 3-21](#) lists the supported APIs and actions.

**Table 3-21** APIs and actions

| API URI                                                   | Request Type | Description                                 | Action                              | Action |
|-----------------------------------------------------------|--------------|---------------------------------------------|-------------------------------------|--------|
| /v1/{project_id}/physicalservers                          | GET          | Batch querying physical servers             | clouddc:imetal:list                 | -      |
| /v1/{project_id}/physicalservers/{id}                     | GET          | Querying information about physical servers | clouddc:imetal:get                  | -      |
| /v1/{project_id}/physicalservers/{id}/hardware-attributes | GET          | Querying server hardware details            | clouddc:imetal:getHardwareAttribute | -      |
| /v1/{project_id}/physicalservers/{id}/firmware-attributes | GET          | Querying server firmware details            | clouddc:imetal:getFirmwareAttribute | -      |

| API URI                                                                | Request Type | Description                                      | Action                                 | Action |
|------------------------------------------------------------------------|--------------|--------------------------------------------------|----------------------------------------|--------|
| /v1/{project_id}/physicalservers/{id}/power-state                      | PUT          | Modifying the power statuses of physical servers | cloudcc:imetal:updatePowerStatus       | -      |
| /v1/{project_id}/physicalservers/{id}/logs/exports                     | POST         | Exporting server logs                            | cloudcc:imetal:createDumpLog           | -      |
| /v1/{project_id}/physicalservers/{id}/logs/exports/{export_id}         | GET          | Querying the export status of logs               | cloudcc:imetal:getDumpLogProgress      | -      |
| /v1/{project_id}/physicalservers/{id}/logs/exports/{export_id}/content | GET          | Downloading logs                                 | cloudcc:imetal:createDownloadLog       | -      |
| /v1/{project_id}/physicalservers/{id}/remote-console-address           | GET          | Obtaining the console address                    | cloudcc:imetal:createRemoteConsoleLink | -      |
| /v1/{project_id}/instances/batch-create                                | POST         | Batch creating instances                         | cloudcc:instance:createBatch           | -      |
| /v1/{project_id}/instances                                             | GET          | Batch querying instances                         | cloudcc:instance:list                  | -      |
| /v1/{project_id}/instances/batch-delete                                | DELETE       | Batch deleting instances                         | cloudcc:instance:deleteBatch           | -      |
| /v1/{project_id}/instance                                              | POST         | Creating an instance                             | cloudcc:instance:create                | -      |
| /v1/{project_id}/instances/{id}                                        | DELETE       | Deleting an instance                             | cloudcc:instance:delete                | -      |



| API URI                                              | Request Type | Description                                    | Action                          | Action |
|------------------------------------------------------|--------------|------------------------------------------------|---------------------------------|--------|
| /v1/{project_id}/instances/{id}/password             | PUT          | Changing the password of an instance           | cloudcc:instance:changePassword | -      |
| /v1/{project_id}/instances/{id}/reinstall            | PUT          | Reinstalling the OS on an instance             | cloudcc:instance:reinstallOS    | -      |
| /v1/{project_id}/instances/{id}/status               | GET          | Querying the status of an instance             | cloudcc:instance:get            | -      |
| /v1/{project_id}/instances/{id}/ip                   | PUT          | Changing the IP address of an instance         | cloudcc:instance:updateIP       | -      |
| /v1/{project_id}/instances/{resource_type}/filter    | POST         | Listing resources                              | cloudcc::listResourcesByTag     | -      |
| /v1/{project_id}/instances/{resource_id}/tags        | GET          | Querying tags of a resource                    | cloudcc::listTagsForResource    | -      |
| /v1/{project_id}/instances/tags                      | GET          | Querying resource tags in a specified project. | cloudcc::listTags               | -      |
| /v1/{project_id}/instances/{resource_type}/count     | POST         | Querying the number of instances               | cloudcc::listResourcesByTag     | -      |
| /v1/{project_id}/instances/{resource_id}/tags/create | POST         | Batch creating resource tags                   | cloudcc::tagResource            | -      |

| API URI                                                    | Request Type | Description                                  | Action                  | Action                |
|------------------------------------------------------------|--------------|----------------------------------------------|-------------------------|-----------------------|
| /v1/{project_id}/{resource_type}/{resource_id}/tags/delete | POST         | Batch deleting resource tags                 | cloudcc::unTagResource  | -                     |
| /v1/{project_id}/physicalservers/status                    | GET          | Obtaining server overview                    | cloudcc::listStatus     | -                     |
| /v1/{project_id}/physicalservers/alarms/summary            | GET          | Obtaining server alarm overview              | cloudcc::listAlarmStat  | ces:alarmHistory:list |
| /v1/{project_id}/physicalservers/alarms/trend              | GET          | Obtaining the server alarm trend             | cloudcc::listAlarmTrend | ces:alarmHistory:list |
| /v1/{project_id}/physicalservers/alarms                    | GET          | Obtaining the server alarm list              | cloudcc::listAlarm      | ces:alarmHistory:list |
| /v1/{project_id}/physicalservers/events                    | GET          | Obtaining the server event list              | cloudcc::listEvent      | ces:events:get        |
| /v1/{project_id}/physicalservers/events/{event_id}         | GET          | Querying event definitions                   | cloudcc::listEventDicts | -                     |
| /v1/{project_id}/repairs                                   | PUT          | Updating or creating server maintenance data | cloudcc::updateRepairs  | -                     |
| /v1/{project_id}/repairs                                   | GET          | Querying server maintenance data             | cloudcc::listRepairs    | -                     |

| API URI                                                              | Request Type | Description                                | Action                       | Action |
|----------------------------------------------------------------------|--------------|--------------------------------------------|------------------------------|--------|
| /v1/{project_id}/spareparts                                          | PUT          | Creating and updating spare parts          | cloudcc::updateSpareParts    | -      |
| /v1/{project_id}/spareparts                                          | GET          | Querying spare parts                       | cloudcc::listSpareParts      | -      |
| /v1/{project_id}/iracks/{irack_id}                                   | PUT          | Modifying the intelligent rack description | cloudcc::irack:update        | -      |
| /v1/{project_id}/iracks                                              | GET          | Querying the intelligent rack list         | cloudcc::irack:list          | -      |
| /v1/{project_id}/idcs                                                | PUT          | Modifying the IDC description              | cloudcc::idc:update          | -      |
| /v1/{project_id}/idcs                                                | GET          | Querying the IDC list                      | cloudcc::idc:list            | -      |
| /v1/{version}/{project_id}/{resource_type}/resource-instances/filter | POST         | Querying the rack list                     | cloudcc::listResourcesByTag  | -      |
| /v1/{version}/{project_id}/{resource_type}/{resource_id}/tags        | GET          | Querying rack tags                         | cloudcc::listTagsForResource | -      |
| /v1/{version}/{project_id}/{resource_type}/tags                      | GET          | Querying rack tags in a specified project  | cloudcc::listTags            | -      |
| /v1/{version}/{project_id}/{resource_type}/resource-instances/count  | POST         | Querying the number of racks               | cloudcc::listResourcesByTag  | -      |

| API URI                                  | Request Type | Description                                    | Action                    | Action |
|------------------------------------------|--------------|------------------------------------------------|---------------------------|--------|
| /v1/{project_id}/iracks/{id}/tags/create | POST         | Batch creating rack tags                       | clouddc::tagResource      | -      |
| /v1/{project_id}/iracks/{id}/tags/delete | POST         | Batch deleting rack tags                       | clouddc::unTagResource    | -      |
| /v1/services/unibuy/extend               | POST         | Granting permissions to check order parameters | clouddc::createIRackOrder | -      |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-22](#), a resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to the resource. If no resource type is specified, the **Resource** element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can specify in identity policy statements for CloudDC.

**Table 3-22** Resource types supported by CloudDC

| Resource Type | URN                                                |
|---------------|----------------------------------------------------|
| iMetal        | clouddc:<region>:<account-id>:imetal:<resource-id> |
| iRack         | clouddc:<region>:<account-id>:irack:<resource-id>  |

## Conditions

### About condition keys

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.

- Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Table 3-23](#). For details about global condition keys, see [Common global condition keys](#).
- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **clouddc:**) only apply to operations of that service. CloudDC does not support service-specific condition keys in identity policies.
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met.

The following table lists the condition keys that you can define in identity policies for CloudDC. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-23** Global condition keys supported by CloudDC

| Global Condition Key                 | Type                 | Description                             |
|--------------------------------------|----------------------|-----------------------------------------|
| <b>g:ResourceTag/&lt;tag-key&gt;</b> | Single-valued string | Tag attached to the requested resource. |
| <b>g:RequestTag/&lt;tag-key&gt;</b>  | Single-valued string | Tag contained in a request.             |
| <b>g:TagKeys</b>                     | Multivalued string   | List of tag keys in a request.          |

## 3.2 Storage

### 3.2.1 Object Storage Service (OBS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational

unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by OBS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by OBS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for OBS.

**Table 3-24** Actions supported by OBS

| Action                          | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|---------------------------------|---------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:object:abortMultipartUpload | Grants the permission to abort multipart uploads. | Write        | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |
|                                 |                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:deleteObject         | Grants the permission to delete an object.        | Write        | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |
|                                 |                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:deleteObjectTagging  | Grants permission to delete object tags.          | Tagging      | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                 |                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

| Action                                | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|---------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:object:deleteObjectVersionTagging | Grants the permission to delete tags of a specified object version. | Tagging      | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">obs:versionId</a></li> </ul>                     | -     |
|                                       |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:deleteObjectVersion        | Grants the permission to delete an object version.                  | Write        | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">obs:versionId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                              | -     |
|                                       |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:getObject                  | Grants the permission to download an object.                        | Read         | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |



| Action                             | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                    |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:getObjectTagging        | Grants the permission to download object tags.                        | Read         | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                    |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:getObjectVersionTagging | Grants the permission to download tags of a specified object version. | Read         | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">obs:versionId</a></li> </ul>                     | -     |
|                                    |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

| Action                         | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|--------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:object:getObjectAcl        | Grants the permission to obtain the ACL of an object.           | Read         | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |
|                                |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:getObjectRetention  | Grants permission to obtain the object retention configuration. | Read         | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |
|                                |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:getObjectVersion    | Grants the permission to download an object version.            | Read         | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">obs:versionId</a></li> </ul>                                                                              | -     |
|                                |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:getObjectVersionAcl | Grants the permission to obtain the ACL of an object version.   | Read         | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">obs:versionId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                              | -     |

| Action                              | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|-------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                     |                                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:listMultipartUploadParts | Grants the permission to obtain all parts associated with a multipart upload.       | List         | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |
|                                     |                                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:modifyObjectMetadata     | Grants the permission to add, modify, or delete the metadata of an existing object. | Write        | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |
|                                     |                                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:putObject                | Grants the permission to upload an object.                                          | Write        | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                           | -     |

| Action                      | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                 | Alias |
|-----------------------------|-------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                             |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:x-obs-acl</a></li> <li>• <a href="#">obs:x-obs-copy-source</a></li> <li>• <a href="#">obs:x-obs-metadata-directive</a></li> <li>• <a href="#">obs:x-obs-server-side-encryption</a></li> </ul> |       |
| obs:object:putObjectTagging | Grants the permission to set object tags. | Tagging      | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                                                                                            | -     |
|                             |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                                                                                                  |       |

| Action                             | Description                                                          | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                | Alias |
|------------------------------------|----------------------------------------------------------------------|-----------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:object:putObjectVersionTagging | Grants the permission to set tags for an object version.             | Tagging               | object *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">obs:versionId</a></li> </ul>                                                                                                                  | -     |
|                                    |                                                                      |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:object:putObjectAcl            | Grants the permission to configure or modify the ACL of an object.   | Permission management | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                        | -     |
|                                    |                                                                      |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:x-obs-acl</a></li> </ul>                                                     |       |
| obs:object:putObjectRetention      | Grants the permission to configure a retention policy for an object. | Write                 | object *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                        | -     |

| Action                         | Description                                                                      | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                            | Alias |
|--------------------------------|----------------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                |                                                                                  |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                          |       |
| obs:object:putObjectVersionAcl | Grants the permission to configure or modify the ACL of an object version.       | Permission_management | object*                     | <ul style="list-style-type: none"> <li>• <a href="#">obs:versionId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                       | -     |
|                                |                                                                                  |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:x-obs-acl</a></li> </ul> |       |
| obs:object:restoreObject       | Grants the permission to restore an object from Archive or Deep Archive storage. | Write                 | object*                     | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                    | -     |
|                                |                                                                                  |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                          |       |
| obs:bucket:createBucket        | Grants the permission to create a bucket.                                        | Write                 | bucket*                     | -                                                                                                                                                                                                                                                        | -     |

| Action                                           | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                            | Alias |
|--------------------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                                  |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:BucketEncrypted</a></li> <li>• <a href="#">obs:x-obs-acl</a></li> </ul> |       |
| obs:bucket:deleteBucket                          | Grants the permission to delete a bucket.                           | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                       | -     |
|                                                  |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                                                                                                                          |       |
| obs:bucket:deleteBucketCustomDomainConfiguration | Grants the permission to delete the custom domain name of a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                       | -     |

| Action                                        | Description                                                              | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|-----------------------------------------------|--------------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                               |                                                                          |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:deleteBucketInventoryConfiguration | Grants the permission to delete the inventory configuration of a bucket. | Write                 | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                               |                                                                          |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:deleteBucketPolicy                 | Grants the permission to delete a bucket policy.                         | Permission_management | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                               |                                                                          |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |



| Action                                         | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:deleteBucketTagging                 | Grants the permission to delete bucket tags.                                                      | Tagging      | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                                |                                                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:deleteBucketWebsite                 | Grants the permission to delete the static website hosting configuration of a bucket.             | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                                |                                                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:deleteDirectColdAccessConfiguration | Grants the permission to delete the direct reading configuration for Archive objects in a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |

| Action                                    | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|-------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                           |                                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:deleteReplicationConfiguration | Grants the permission to delete the replication configuration of a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                           |                                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketAcl                   | Grants the permission to obtain the bucket ACL.                            | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                           |                                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

| Action                                        | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|-----------------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:getBucketObjectLockConfiguration   | Grants the permission to query the default WORM policy and retention period for a bucket. | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                               |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketCORS                      | Grants the permission to query the CORS configuration of a bucket.                        | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                               |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketCustomDomainConfiguration | Grants the permission to query the custom domain name of a bucket.                        | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |

| Action                                     | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|--------------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                            |                                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketInventoryConfiguration | Grants the permission to query the inventory configuration of a bucket. | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                            |                                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketLocation               | Grants the permission to query the location of a bucket.                | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                            |                                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

| Action                      | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|-----------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:getBucketLogging | Grants the permission to query the logging configuration of a bucket. | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                             |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketPolicy  | Grants the permission to obtain a bucket policy.                      | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                             |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketQuota   | Grants the permission to obtain the storage quota of a bucket.        | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |

| Action                            | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|-----------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                   |                                                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketStorage       | Grants the permission to query the object count and storage usage of a bucket. | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                   |                                                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketStoragePolicy | Grants the permission to obtain the default storage class of a bucket.         | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                   |                                                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

| Action                         | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|--------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:getBucketTagging    | Grants the permission to obtain bucket tags.                                          | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                |                                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketVersioning | Grants the permission to obtain the versioning status of a bucket.                    | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                |                                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketWebsite    | Grants the permission to obtain the static website hosting configuration of a bucket. | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |

| Action                                      | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|---------------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                             |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getDirectColdAccessConfiguration | Grants the permission to obtain the direct reading policy of Archive objects in a bucket. | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                             |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getEncryptionConfiguration       | Grants the permission to obtain the encryption configuration of a bucket.                 | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                             |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |



| Action                                 | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|----------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:getLifecycleConfiguration   | Grants the permission to obtain the lifecycle configuration of a bucket.                | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                        |                                                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getReplicationConfiguration | Grants the permission to obtain the cross-region replication configuration of a bucket. | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                        |                                                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:headBucket                  | Grants the permission to obtain the metadata of a bucket.                               | Read         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |

| Action                      | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                          | Alias |
|-----------------------------|--------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                             |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                                                                                                        |       |
| obs:bucket:listAllMyBuckets | Grants the permission to list the created buckets.     | List         | bucket *                    | -                                                                                                                                                                                                                                                                                                                                      |       |
|                             |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                                                                                                        |       |
| obs:bucket:listBucket       | Grants the permission to list the objects in a bucket. | List         | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                     |       |
|                             |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:prefix</a></li> <li>• <a href="#">obs:delimiter</a></li> <li>• <a href="#">obs:max-keys</a></li> </ul> |       |

| Action                                | Description                                                                | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                          | Alias |
|---------------------------------------|----------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:listBucketMultipartUploads | Grants the permission to list the initiated multipart uploads in a bucket. | List                  | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                     | -     |
|                                       |                                                                            |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                                                                                                        |       |
| obs:bucket:listBucketVersions         | Grants the permission to list the object versions in a bucket.             | List                  | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                     | -     |
|                                       |                                                                            |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:prefix</a></li> <li>• <a href="#">obs:delimiter</a></li> <li>• <a href="#">obs:max-keys</a></li> </ul> |       |
| obs:bucket:putBucketAcl               | Grants the permission to configure an ACL for a bucket.                    | Permission_management | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                     | -     |

| Action                                        | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                            | Alias |
|-----------------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                               |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:x-obs-acl</a></li> </ul> |       |
| obs:bucket:putBucketCORS                      | Grants the permission to configure CORS for a bucket.                 | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                       | -     |
|                                               |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                          |       |
| obs:bucket:putBucketCustomDomainConfiguration | Grants the permission to configure a custom domain name for a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                       | -     |
|                                               |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                          |       |

| Action                                      | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|---------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:putBucketObjectLockConfiguration | Grants the permission to configure a default WORM policy for a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                             |                                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putBucketInventoryConfiguration  | Grants the permission to configure an inventory rule for a bucket.     | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                             |                                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putBucketLogging                 | Grants the permission to configure logging for a bucket.               | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |

| Action                     | Description                                                | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|----------------------------|------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                            |                                                            |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putBucketPolicy | Grants the permission to configure a bucket policy.        | Permission_management | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                            |                                                            |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putBucketQuota  | Grants the permission to set a storage quota for a bucket. | Write                 | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                            |                                                            |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

| Action                            | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                | Alias |
|-----------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:putBucketStoragePolicy | Grants the permission to configure a default storage class for a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                           | -     |
|                                   |                                                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                                                                              |       |
| obs:bucket:putBucketTagging       | Grants the permission to configure tags for a bucket.                    | Tagging      | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                           | -     |
|                                   |                                                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putBucketVersioning    | Grants the permission to configure versioning for a bucket.              | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                           | -     |

| Action                                      | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|---------------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                             |                                                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putBucketWebsite                 | Grants the permission to configure static website hosting for a bucket.            | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                             |                                                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putDirectColdAccessConfiguration | Grants the permission to configure direct reading for Archive objects in a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                             |                                                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |



| Action                                 | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                  | Alias |
|----------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:putEncryptionConfiguration  | Grants the permission to configure bucket encryption.                     | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                             | -     |
|                                        |                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> <li>• <a href="#">obs:BucketEncrypted</a></li> </ul> |       |
| obs:bucket:putLifecycleConfiguration   | Grants the permission to configure a lifecycle rule for a bucket.         | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                             | -     |
|                                        |                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul>                                                |       |
| obs:bucket:putReplicationConfiguration | Grants the permission to configure cross-region replication for a bucket. | Write        | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                             | -     |

| Action                                | Description                                                        | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|---------------------------------------|--------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                       |                                                                    |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketPublicAccessBlock | Grants the permission to obtain the BPA configuration of a bucket. | Read                  | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                       |                                                                    |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:putBucketPublicAccessBlock | Grants the permission to configure BPA for a bucket.               | Permission_management | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                       |                                                                    |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

| Action                                   | Description                                                           | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|------------------------------------------|-----------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| obs:bucket:deleteBucketPublicAccessBlock | Grants the permission to delete the BPA configuration of a bucket.    | Permission_management | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                          |                                                                       |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketPolicyPublicStatus   | Grants the permission to obtain the public status of a bucket policy. | Read                  | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |
|                                          |                                                                       |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |
| obs:bucket:getBucketPublicStatus         | Grants the permission to obtain the public status of a bucket.        | Read                  | bucket *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                              | -     |

| Action | Description | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                   | Alias |
|--------|-------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|        |             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">obs:EpochTime</a></li> <li>• <a href="#">obs:SourceIp</a></li> <li>• <a href="#">obs:TlsVersion</a></li> <li>• <a href="#">obs:CustomDomain</a></li> </ul> |       |

Each API of OBS usually supports one or more actions. [Table 3-25](#) lists the supported actions and dependencies.

**Table 3-25** Actions and dependencies supported by OBS APIs

| API                      | Action                                    | Dependencies |
|--------------------------|-------------------------------------------|--------------|
| PUT /?replication        | obs:bucket:putReplicationConfiguration    | -            |
| GET /?replication        | obs:bucket:getReplicationConfiguration    | -            |
| DELETE /?replication     | obs:bucket:deleteReplicationConfiguration | -            |
| PUT /ObjectName?acl      | obs:object:putObjectAcl                   | -            |
| PUT /ObjectName?acl      | obs:object:putObjectVersionAcl            | -            |
| GET /ObjectName?acl      | obs:object:getObjectAcl                   | -            |
| GET /ObjectName?acl      | obs:object:getObjectVersionAcl            | -            |
| PUT /ObjectName?metadata | obs:object:modifyObjectMetadata           | -            |

| API                                         | Action                             | Dependencies                                                                                                                                                                                                                                    |
|---------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /                                      | obs:object:putObject               | <ul style="list-style-type: none"> <li>• kms:cmk:create</li> <li>• kms:cmk:list</li> <li>• kms:cmk:createDataKey</li> <li>• functiongraph:function:invokeAsync</li> <li>• functiongraph:workflow:invoke</li> <li>• smn:topic:publish</li> </ul> |
| PUT /ObjectName                             | obs:object:putObject               | <ul style="list-style-type: none"> <li>• kms:cmk:create</li> <li>• kms:cmk:list</li> <li>• kms:cmk:createDataKey</li> <li>• functiongraph:function:invokeAsync</li> <li>• functiongraph:workflow:invoke</li> <li>• smn:topic:publish</li> </ul> |
| PUT /objectname?tagging&versionId=versionid | obs:object:putObjectTagging        | -                                                                                                                                                                                                                                               |
| PUT /objectName?tagging&versionId           | obs:object:putObjectVersionTagging | -                                                                                                                                                                                                                                               |
| GET /ObjectName                             | obs:object:getObject               | <ul style="list-style-type: none"> <li>• kms:cmk:create</li> <li>• kms:cmk:list</li> <li>• kms:cmk:decryptDataKey</li> </ul>                                                                                                                    |
| GET /objectname?tagging&versionId=versionid | obs:object:getObjectTagging        | -                                                                                                                                                                                                                                               |
| GET /objectName?tagging&versionId           | obs:object:getObjectVersionTagging | -                                                                                                                                                                                                                                               |
| GET /ObjectName                             | obs:object:getObjectVersion        | <ul style="list-style-type: none"> <li>• kms:cmk:create</li> <li>• kms:cmk:list</li> <li>• kms:cmk:decryptDataKey</li> </ul>                                                                                                                    |
| HEAD /ObjectName                            | obs:object:getObject               | obs:object:getObjectRetention                                                                                                                                                                                                                   |
| HEAD /ObjectName                            | obs:object:getObjectVersion        | obs:object:getObjectRetention                                                                                                                                                                                                                   |

| API                                                                                           | Action                                | Dependencies                                                                                                                                           |
|-----------------------------------------------------------------------------------------------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /<br>ObjectName                                                                        | obs:object:deleteObject               | <ul style="list-style-type: none"> <li>functiongraph:function:invokeAsync</li> <li>functiongraph:workflow:invoke</li> <li>smn:topic:publish</li> </ul> |
| DELETE /<br>objectname?<br>tagging&versionId=<br>versionid                                    | obs:object:deleteObjectTagging        | -                                                                                                                                                      |
| DELETE /<br>objectName?<br>tagging&versionId                                                  | obs:object:deleteObjectVersionTagging | -                                                                                                                                                      |
| DELETE /<br>ObjectName                                                                        | obs:object:deleteObjectVersion        | <ul style="list-style-type: none"> <li>functiongraph:function:invokeAsync</li> <li>functiongraph:workflow:invoke</li> <li>smn:topic:publish</li> </ul> |
| POST /<br>ObjectName?<br>uploads                                                              | obs:object:putObject                  | <ul style="list-style-type: none"> <li>kms:cmk:create</li> <li>kms:cmk:list</li> <li>kms:cmk:createDataKey</li> </ul>                                  |
| GET /?<br>uploads&max-<br>uploads=max                                                         | obs:bucket:listBucketMultipartUploads | -                                                                                                                                                      |
| PUT /ObjectName?<br>partNumber=partN<br>um&uploadId=uplo<br>adID                              | obs:object:putObject                  | <ul style="list-style-type: none"> <li>kms:cmk:createDataKey</li> <li>kms:cmk:decryptDataKey</li> </ul>                                                |
| GET /ObjectName?<br>uploadId=uploadid&<br>max-<br>parts=max&part-<br>number-<br>marker=marker | obs:object:listMultipartUploadParts   | -                                                                                                                                                      |
| DELETE /<br>ObjectName?<br>uploadId=uplaodID                                                  | obs:object:abortMultipartUpload       | -                                                                                                                                                      |
| POST /<br>ObjectName?<br>uploadId=uploadID                                                    | obs:object:putObject                  | <ul style="list-style-type: none"> <li>functiongraph:function:invokeAsync</li> <li>functiongraph:workflow:invoke</li> <li>smn:topic:publish</li> </ul> |

| API                                                  | Action                                         | Dependencies |
|------------------------------------------------------|------------------------------------------------|--------------|
| PUT /?website                                        | obs:bucket:putBucketWebsite                    | -            |
| GET /?website                                        | obs:bucket:getBucketWebsite                    | -            |
| DELETE /?website                                     | obs:bucket:deleteBucketWebsite                 | -            |
| PUT /?cors                                           | obs:bucket:putBucketCORS                       | -            |
| GET /?cors                                           | obs:bucket:getBucketCORS                       | -            |
| DELETE /?cors                                        | obs:bucket:putBucketCORS                       | -            |
| PUT /?directcoldaccess                               | obs:bucket:putDirectColdAccessConfiguration    | -            |
| GET /?directcoldaccess                               | obs:bucket:getDirectColdAccessConfiguration    | -            |
| DELETE /?directcoldaccess                            | obs:bucket:deleteDirectColdAccessConfiguration | -            |
| POST /<br>ObjectName?<br>restore&versionId=VersionID | obs:object:restoreObject                       | -            |
| PUT /?quota                                          | obs:bucket:putBucketQuota                      | -            |
| GET /?quota                                          | obs:bucket:getBucketQuota                      | -            |
| PUT /?lifecycle                                      | obs:bucket:putLifecycleConfiguration           | -            |
| DELETE /?lifecycle                                   | obs:bucket:putLifecycleConfiguration           | -            |
| GET /?lifecycle                                      | obs:bucket:getLifecycleConfiguration           | -            |
| PUT /?acl                                            | obs:bucket:putBucketAcl                        | -            |
| GET /?acl                                            | obs:bucket:getBucketAcl                        | -            |
| PUT /?logging                                        | obs:bucket:putBucketLogging                    | -            |
| GET /?logging                                        | obs:bucket:getBucketLogging                    | -            |
| PUT /?tagging                                        | obs:bucket:putBucketTagging                    | -            |
| GET /?tagging                                        | obs:bucket:getBucketTagging                    | -            |

| API                                    | Action                                        | Dependencies |
|----------------------------------------|-----------------------------------------------|--------------|
| DELETE /?tagging                       | obs:bucket:deleteBucketTagging                | -            |
| PUT /?policy                           | obs:bucket:putBucketPolicy                    | -            |
| GET /?policy                           | obs:bucket:getBucketPolicy                    | -            |
| DELETE /?policy                        | obs:bucket:deleteBucketPolicy                 | -            |
| GET /?storageinfo                      | obs:bucket:getBucketStorage                   | -            |
| PUT /                                  | obs:bucket:createBucket                       | -            |
| DELETE /                               | obs:bucket:deleteBucket                       | -            |
| HEAD /                                 | obs:bucket:headBucket                         | -            |
| GET /                                  | obs:bucket:listBucket                         | -            |
| GET /?location                         | obs:bucket:getBucketLocation                  | -            |
| PUT /?versioning                       | obs:bucket:putBucketVersioning                | -            |
| GET /?versioning                       | obs:bucket:getBucketVersioning                | -            |
| GET /                                  | obs:bucket:listBucketVersions                 | -            |
| PUT /?encryption                       | obs:bucket:putEncryptionConfiguration         | kms:cmk:get  |
| GET /?encryption                       | obs:bucket:getEncryptionConfiguration         | -            |
| DELETE /?encryption                    | obs:bucket:putEncryptionConfiguration         | -            |
| PUT /?inventory&id=configuration-id    | obs:bucket:putBucketInventoryConfiguration    | -            |
| GET /?inventory&id=configuration-id    | obs:bucket:getBucketInventoryConfiguration    | -            |
| GET /?inventory                        | obs:bucket:getBucketInventoryConfiguration    | -            |
| DELETE /?inventory&id=configuration-id | obs:bucket:deleteBucketInventoryConfiguration | -            |



| API                                                     | Action                                           | Dependencies                                                                                                                                                                        |
|---------------------------------------------------------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /?storageClass                                      | obs:bucket:putBucketStoragePolicy                | -                                                                                                                                                                                   |
| GET /?storageClass                                      | obs:bucket:getBucketStoragePolicy                | -                                                                                                                                                                                   |
| PUT /?customdomain=domainname                           | obs:bucket:putBucketCustomDomainConfiguration    | -                                                                                                                                                                                   |
| GET /?customdomain                                      | obs:bucket:getBucketCustomDomainConfiguration    | -                                                                                                                                                                                   |
| DELETE /?customdomain=domainname                        | obs:bucket:deleteBucketCustomDomainConfiguration | -                                                                                                                                                                                   |
| PUT /?object-lock                                       | obs:bucket:putBucketObjectLockConfiguration      | -                                                                                                                                                                                   |
| GET /?object-lock                                       | obs:bucket:getBucketObjectLockConfiguration      | -                                                                                                                                                                                   |
| PUT /ObjectName?retention&versionId=versionid           | obs:object:putObjectRetention                    | -                                                                                                                                                                                   |
| PUT /ObjectName?partNumber=partNumber&uploadId=UploadID | obs:object:putObject                             | <ul style="list-style-type: none"> <li>obs:object:getObject</li> <li>kms:cmk:create</li> <li>kms:cmk:list</li> <li>kms:cmk:createDataKey</li> <li>kms:cmk:decryptDataKey</li> </ul> |
| POST /?delete                                           | obs:object:deleteObject                          | <ul style="list-style-type: none"> <li>functiongraph:function:invokeAsync</li> <li>functiongraph:workflow:invoke</li> <li>smn:topic:publish</li> </ul>                              |

| API                                               | Action                                   | Dependencies                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /<br>destinationObject-<br>Name               | obs:object:putObject                     | <ul style="list-style-type: none"> <li>obs:object:getObject</li> <li>kms:cmk:create</li> <li>kms:cmk:list</li> <li>kms:cmk:createDataKey</li> <li>kms:cmk:decryptDataKey</li> <li>functiongraph:function:invokeAsync</li> <li>functiongraph:workflow:invoke</li> <li>smn:topic:publish</li> </ul> |
| GET /                                             | obs:bucket:listAllMyBuckets              | -                                                                                                                                                                                                                                                                                                 |
| PUT /ObjectName?<br>truncate&length=Length        | obs:object:putObject                     | -                                                                                                                                                                                                                                                                                                 |
| POST /<br>ObjectName?<br>append&position=Position | obs:object:putObject                     | <ul style="list-style-type: none"> <li>kms:cmk:create</li> <li>kms:cmk:list</li> <li>kms:cmk:createDataKey</li> <li>kms:cmk:decryptDataKey</li> </ul>                                                                                                                                             |
| PUT /ObjectName?<br>modify&position=Position      | obs:object:putObject                     | -                                                                                                                                                                                                                                                                                                 |
| POST /<br>ObjectName?<br>name=Name&rename         | obs:object:getObject                     | obs:object:putObject                                                                                                                                                                                                                                                                              |
| GET /?<br>publicAccessBlock                       | obs:bucket:getBucketPublicAccessBlock    | -                                                                                                                                                                                                                                                                                                 |
| PUT /?<br>publicAccessBlock                       | obs:bucket:putBucketPublicAccessBlock    | -                                                                                                                                                                                                                                                                                                 |
| DELETE /?<br>publicAccessBlock                    | obs:bucket:deleteBucketPublicAccessBlock | -                                                                                                                                                                                                                                                                                                 |
| GET /?policyStatus                                | obs:bucket:getBucketPolicy-PublicStatus  | -                                                                                                                                                                                                                                                                                                 |
| GET /?bucketStatus                                | obs:bucket:getBucketPublic-Status        | -                                                                                                                                                                                                                                                                                                 |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-26](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for OBS.

**Table 3-26** Resource types supported by OBS

| Resource Type | URN                                      |
|---------------|------------------------------------------|
| bucket        | obs:::bucket:<bucket-name>               |
| object        | obs:::object:<bucket-name>/<object-name> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, obs) apply only to operations of the xx service. For details, see [Table 3-27](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
  - A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by OBS

The following table lists the condition keys that you can define in identity policies for OBS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-27** Service-specific condition keys supported by OBS

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                                                                                                           |
|--------------------------------|---------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| obs:versionId                  | string  | Single-valued                 | Filters requests by the object version ID.                                                                                                                            |
| obs:prefix                     | string  | Single-valued                 | Filters requests by the prefix specified for objects to be listed.                                                                                                    |
| obs:delimiter                  | string  | Single-valued                 | Filters requests by the delimiter character for grouping objects.                                                                                                     |
| obs:max-keys                   | numeric | Single-valued                 | Filters requests by the maximum number of objects to return. The max-keys parameter indicates how many objects can be returned at most in alphabetical order.         |
| obs:x-obs-acl                  | string  | Single-valued                 | Filters requests by the ACL header. The ACL value can be private, public-read, public-read-write, bucketowner-read, bucket-owner-full-control, or log-delivery-write. |
| obs:x-obs-copy-source          | string  | Single-valued                 | Filters requests by the source bucket and object used for replication. The format is /bucketname/keyname.                                                             |

| Service-specific Condition Key   | Type       | Single-valued/<br>Multivalued | Description                                                                                                                                                                   |
|----------------------------------|------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| obs:x-obs-metadata-directive     | string     | Single-valued                 | Filters requests by whether the metadata of the destination object is copied from the source object or replaced with the metadata contained in the request (COPY or REPLACE). |
| obs:x-obs-server-side-encryption | string     | Single-valued                 | Filters requests by whether objects in the bucket are encrypted. The value is kms.                                                                                            |
| obs:SourceIp                     | ip_address | Single-valued                 | Filters requests by the first IP address in the x-forward-for header or the source IP address of the request.                                                                 |
| obs:EpochTime                    | numeric    | Single-valued                 | Filters requests by the time when the request is received by the server, which is the number of non-leap seconds that have elapsed since 1970.01.01 00:00:00 UTC.             |
| obs:BucketEncrypted              | boolean    | Single-valued                 | Filters requests by the encryption status of the bucket after the bucket is created, encrypted, or decrypted.                                                                 |
| obs:TlsVersion                   | numeric    | Single-valued                 | Filters requests by the TLS protocol version used by the client.                                                                                                              |
| obs:CustomDomain                 | boolean    | Single-valued                 | Filters requests by whether the requester client uses a custom domain name.                                                                                                   |

## 3.2.2 Cloud Backup and Recovery (CBR)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CBR, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CBR, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CBR.

**Table 3-28** Actions supported by CBR

| Action                       | Description                                         | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                              |
|------------------------------|-----------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------|
| cbr:backups:getMetadata      | Grants permission to get backup metadata.           | Read         | backup *                    | -             | -                                                                                  |
| cbr::getAgentAutoUpgrade     | Grants permission to get agent auto upgrade status. | Read         | -                           | -             | <ul style="list-style-type: none"> <li>• cbr:agents:getAgentAutoUpgrade</li> </ul> |
| cbr::updateSnapshotMetadata  | Grants permission to update snapshot metadata.      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>• cbr:snapshotMetadata:update</li> </ul>    |
| cbr::updateThirdAuth         | Grants permission to update third auth.             | Write        | -                           | -             | <ul style="list-style-type: none"> <li>• cbr:thirdAuth:update</li> </ul>           |
| cbr::setAgentAutoUpgrade     | Grants permission to set agent auto upgrade status. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>• cbr:agents:setAgentAutoUpgrade</li> </ul> |
| cbr::readBucketAuthorization | Grants permission to read bucket authorization.     | Read         | -                           | -             | <ul style="list-style-type: none"> <li>• cbr:bucketAuthorization:read</li> </ul>   |
| cbr::listExportSnapshotJob   | Grants permission to create export snapshot job.    | List         | -                           | -             | <ul style="list-style-type: none"> <li>• cbr:exportSnapshotJob:list</li> </ul>     |

| Action                          | Description                                         | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                             |
|---------------------------------|-----------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------|
| cbr::listThirdAuth              | Grants permission to list third auth.               | List         | -                           | -             | <ul style="list-style-type: none"> <li>cbr:thirdAuth:list</li> </ul>              |
| cbr::listFeatures               | Grants permission to list features.                 | Read         | -                           | -             | <ul style="list-style-type: none"> <li>cbr:features:list</li> </ul>               |
| cbr::listExportSnapshotAgency   | Grants permission to list export snapshot agency.   | List         | -                           | -             | <ul style="list-style-type: none"> <li>cbr:exportSnapshotAgency:list</li> </ul>   |
| cbr::getThirdAuth               | Grants permission to get third auth.                | Read         | -                           | -             | <ul style="list-style-type: none"> <li>cbr:thirdAuth:get</li> </ul>               |
| cbr::getFeature                 | Grants permission to get feature.                   | Read         | -                           | -             | <ul style="list-style-type: none"> <li>cbr:feature:get</li> </ul>                 |
| cbr::getExportSnapshotJob       | Grants permission to list export snapshot job.      | Read         | -                           | -             | <ul style="list-style-type: none"> <li>cbr:exportSnapshotJob:get</li> </ul>       |
| cbr::deleteThirdAuth            | Grants permission to delete third auth.             | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cbr:thirdAuth:delete</li> </ul>            |
| cbr::deleteExportSnapshotAgency | Grants permission to delete export snapshot agency. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cbr:exportSnapshotAgency:delete</li> </ul> |
| cbr::deleteExportSnapshotJob    | Grants permission to delete export snapshot job.    | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cbr:exportSnapshotJob:delete</li> </ul>    |



| Action                          | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                                                                             |
|---------------------------------|-------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| cbr::createExportSnapshotAgency | Grants permission to create export snapshot agency.   | Write        | -                           | -                                                                                                              | <ul style="list-style-type: none"> <li>cbr:exportSnapshotAgency:create</li> </ul> |
| cbr::createSnapshotMetadata     | Grants permission to create snapshot metadata.        | Write        | -                           | -                                                                                                              | <ul style="list-style-type: none"> <li>cbr:snapshotMetadata:create</li> </ul>     |
| cbr::createThirdAuth            | Grants permission to create third auth.               | Write        | -                           | -                                                                                                              | <ul style="list-style-type: none"> <li>cbr:thirdAuth:create</li> </ul>            |
| cbr::createExportSnapshotJob    | Grants permission to create export snapshot job.      | Write        | -                           | -                                                                                                              | <ul style="list-style-type: none"> <li>cbr:exportSnapshotJob:create</li> </ul>    |
| cbr::createBucketAuthorization  | Grants permission to create bucket authorization.     | Write        | -                           | -                                                                                                              | <ul style="list-style-type: none"> <li>cbr:bucketAuthorization:create</li> </ul>  |
| cbr:tasks:list                  | Grants permission to query task list.                 | List         | task *                      | -                                                                                                              | -                                                                                 |
|                                 |                                                       |              | -                           | g:EnterpriseProjectId                                                                                          |                                                                                   |
| cbr::vaults:changeChargeMode    | Grants permission to change the charge mode of vault. | Write        | vault *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -                                                                                 |
| cbr::rackGroups:create          | Grants permission to create rack groups.              | Write        | rackGroup *                 | -                                                                                                              | -                                                                                 |
| cbr::rackGroups:list            | Grants permission to list rack groups.                | Read         | rackGroup *                 | -                                                                                                              | -                                                                                 |

| Action                    | Description                                       | Access Level          | Resource Type (*: required) | Condition Key                         | Alias |
|---------------------------|---------------------------------------------------|-----------------------|-----------------------------|---------------------------------------|-------|
| cbr:backups:import        | Grants permission to import backup.               | Write                 | vault *                     | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:tasks:get             | Grants permission to query a task.                | Read                  | task *                      | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:member:create         | Grants permission to add backup member.           | Permission_management | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
|                           |                                                   |                       | -                           | <a href="#">cbr:TargetOrgPaths</a>    |       |
| cbr:member:update         | Grants permission to update backup member status. | Write                 | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:member:get            | Grants permission to get backup member details.   | Read                  | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:member:list           | Grants permission to list backup members.         | List                  | backup *                    | -                                     | -     |
| cbr:member:delete         | Grants permission to delete backup member.        | Permission_management | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:vaults:showCheckpoint | Grants permission to get checkpoint.              | Read                  | -                           | -                                     | -     |

| Action                  | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                  | Alias |
|-------------------------|---------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cbr:vaults:syncCapacity | Grants permission to update vault capacity. | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                             | -     |
| cbr:vaults:showSummary  | Grants permission to show vault summary.    | List         | -                           | -                                                                                                                                                                                                                              | -     |
| cbr:vaults:replicate    | Grants permission to replicate checkpoint.  | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                             | -     |
| cbr:vaults:backup       | Grants permission to create checkpoint.     | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                             | -     |
| cbr:vaults:sync         | Grants permission to sync checkpoint.       | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                             | -     |
| cbr:vaults:create       | Grants permission to create vault.          | Write        | vault *                     | -                                                                                                                                                                                                                              | -     |
|                         |                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">cbr:PolicyId</a></li> </ul> |       |

| Action                     | Description                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------|----------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cbr:vaults:get             | Grants permission to get vault.        | Read         | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:vaults:list            | Grants permission to list vaults.      | List         | vault *                     | -                                                                                                                                                  | -     |
|                            |                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| cbr:vaults:update          | Grants permission to modify vault.     | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:vaults:delete          | Grants permission to delete vault.     | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:vaults:removeResources | Grants permission to remove resources. | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:vaults:addResources    | Grants permission to add resources.    | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                        | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------|--------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cbr:vaults:setResources       | Grants permission to set resources.        | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:vaults:associatePolicy    | Grants permission to associate policy.     | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:vaults:dissociatePolicy   | Grants permission to dissociate policy.    | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:vaults:listExternalVaults | Grants permission to list external vaults. | List         | vault *                     | -                                                                                                                                                  | -     |
| cbr:vaults:migrateResources   | Grants permission to migrate resources.    | Write        | vault *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:backups:sync              | Grants permission to sync backups.         | Write        | vault *                     | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -     |
| cbr:backups:get               | Grants permission to get backup.           | Read         | backup *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -     |
| cbr:backups:showMetadata      | Grants permission to get backup metadata.  | Read         | backup *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -     |

| Action                | Description                            | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|-----------------------|----------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| cbr:backups:list      | Grants permission to list backups.     | List         | backup *                    | -                                     | -     |
|                       |                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| cbr:backups:delete    | Grants permission to delete backup.    | Write        | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:backups:replicate | Grants permission to replicate backup. | Write        | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:backups:restore   | Grants permission to restore backup.   | Write        | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:backups:update    | Grants permission to update backup.    | Write        | backup *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cbr:policies:list     | Grants permission to list policies.    | List         | policy *                    | -                                     | -     |
| cbr:policies:create   | Grants permission to create policy.    | Write        | policy *                    | -                                     | -     |
|                       |                                        |              | -                           | <a href="#">cbr:EnabledPolicy</a>     |       |
| cbr:policies:get      | Grants permission to get policy.       | Read         | policy *                    | -                                     | -     |
| cbr:policies:update   | Grants permission to modify policy.    | Write        | policy *                    | -                                     | -     |
|                       |                                        |              | -                           | <a href="#">cbr:EnabledPolicy</a>     |       |
| cbr:policies:delete   | Grants permission to delete policy.    | Write        | policy *                    | -                                     | -     |

| Action                                 | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|----------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| cbr:vaults:listProtectables            | Grants permission to list protectables.                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             | -     |
| cbr:vaults:getProtectables             | Grants permission to get protectable.                       | Read         | -                           | -                                                                                                                                 | -     |
| cbr:backups:queryReplicationCapability | Grants permission to query replication capability.          | List         | -                           | -                                                                                                                                 | -     |
| cbr:backups:checkAgent                 | Grants permission to check agent status.                    | Read         | -                           | -                                                                                                                                 | -     |
| cbr:vaults:listResourceInstances       | Grants permission to list resource instances.               | List         | vault *                     | -                                                                                                                                 | -     |
| cbr:vaults:bulkCreateOrDeleteTags      | Grants permission to bulk create or delete tags of a vault. | Write        | vault *                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                        |                                                             |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| cbr:vaults:setTags                     | Grants permission to set tags of a vault.                   | Write        | vault *                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                        |                                                             |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| cbr:vaults:deleteTags                  | Grants permission to delete tags of a vault.                | Write        | vault *                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                        |                                                             |              | -                           | <a href="#">g:TagKeys</a>                                                                                                         |       |

| Action                       | Description                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias |
|------------------------------|-----------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cbr:vaults:getTags           | Grants permission to get tags of a vault.     | Read         | vault *                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -     |
| cbr:vaults:listProjectTags   | Grants permission to list resource instances. | List         | vault *                     | -                                                                                                                                              | -     |
| cbr:backups:listStorageUsage | Grants permission to list storage usage.      | List         | -                           | -                                                                                                                                              | -     |
| cbr:vaults:updateOrder       | Grants permission to update order.            | Write        | vault *                     | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cbr:agents:addPath           | Grants permission to add path.                | Write        | agent *                     | -                                                                                                                                              | -     |
| cbr:agents:get               | Grants permission to get agent.               | Read         | agent *                     | -                                                                                                                                              | -     |
| cbr:agents:update            | Grants permission to update agent.            | Write        | agent *                     | -                                                                                                                                              | -     |
| cbr:agents:register          | Grants permission to register agent.          | Write        | agent *                     | -                                                                                                                                              | -     |
| cbr:agents:delete            | Grants permission to delete agent.            | Write        | agent *                     | -                                                                                                                                              | -     |
| cbr:agents:removePath        | Grants permission to remove path.             | Write        | agent *                     | -                                                                                                                                              | -     |



| Action                                    | Description                                          | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------------------|------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| cbr:agents:list                           | Grants permission to list agents.                    | List         | agent *                     | -             | -     |
| cbr:backups:migratesCreate                | Grants permission to migrates.                       | Write        | -                           | -             | -     |
| cbr:backups:migratesIndex                 | Grants permission to get migrates.                   | Read         | -                           | -             | -     |
| cbr:organizationPolicies:create           | Grants permission to create organization Policies.   | Write        | -                           | -             | -     |
| cbr:organizationPolicies:listPolicyDetail | Grants permission to get organization policy detail. | Read         | -                           | -             | -     |
| cbr:organizationPolicies:delete           | Grants permission to delete organization policy.     | Write        | -                           | -             | -     |
| cbr:organizationPolicies:update           | Grants permission to modify organization policy.     | Write        | -                           | -             | -     |
| cbr:organizationPolicies:list             | Grants permission to list organization policies.     | List         | -                           | -             | -     |
| cbr:organizationPolicies:get              | Grants permission to get organization policy.        | Read         | -                           | -             | -     |

Each API of CBR usually supports one or more actions. [Table 3-29](#) lists the supported actions and dependencies.

**Table 3-29** Actions and dependencies supported by CBR APIs

| API                                                          | Action                      | Dependencies |
|--------------------------------------------------------------|-----------------------------|--------------|
| GET /v3/{project_id}/cbr-features                            | cbr::listFeatures           | -            |
| GET /v3/{project_id}/cbr-features/{feature_key}              | cbr::getFeature             | -            |
| POST /v3/{project_id}/vaults/change-charge-mode              | cbr:vaults:changeChargeMode | -            |
| GET /v3/{project_id}/operation-logs                          | cbr:tasks:list              | -            |
| GET /v3/{project_id}/operation-logs/{operation_log_id}       | cbr:tasks:get               | -            |
| POST /v3/{project_id}/backups/{backup_id}/members            | cbr:member:create           | -            |
| PUT /v3/{project_id}/backups/{backup_id}/members/{member_id} | cbr:member:update           | -            |
| GET /v3/{project_id}/backups/{backup_id}/members/{member_id} | cbr:member:get              | -            |
| GET /v3/{project_id}/backups/{backup_id}/members             | cbr:member:list             | -            |

| API                                                                                 | Action                    | Dependencies                                                                                                        |
|-------------------------------------------------------------------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------|
| DELETE /v3/<br>{project_id}/<br>backups/<br>{backup_id}/<br>members/<br>{member_id} | cbr:member:delete         | -                                                                                                                   |
| GET /v3/<br>{project_id}/<br>checkpoints/<br>{checkpoint_id}                        | cbr:vaults:showCheckpoint | -                                                                                                                   |
| GET /v3/<br>{project_id}/vaults/<br>summary                                         | cbr:vaults:showSummary    | -                                                                                                                   |
| POST /v3/<br>{project_id}/<br>checkpoints/<br>replicate                             | cbr:vaults:replicate      | -                                                                                                                   |
| POST /v3/<br>{project_id}/<br>checkpoints                                           | cbr:vaults:backup         | <ul style="list-style-type: none"> <li>• ecs:cloudServers:listServersDetails</li> <li>• evs:volumes:list</li> </ul> |
| POST /v3/<br>{project_id}/<br>checkpoints/sync                                      | cbr:vaults:sync           | -                                                                                                                   |
| POST /v3/<br>{project_id}/vaults                                                    | cbr:vaults:create         | <ul style="list-style-type: none"> <li>• ecs:cloudServers:listServersDetails</li> <li>• evs:volumes:list</li> </ul> |
| POST /v3/<br>{project_id}/vaults/<br>order                                          | cbr:vaults:create         | <ul style="list-style-type: none"> <li>• ecs:cloudServers:listServersDetails</li> <li>• evs:volumes:list</li> </ul> |
| GET /v3/<br>{project_id}/vaults/<br>{vault_id}                                      | cbr:vaults:get            | -                                                                                                                   |
| GET /v3/<br>{project_id}/vaults                                                     | cbr:vaults:list           | -                                                                                                                   |
| PUT /v3/<br>{project_id}/vaults/<br>{vault_id}                                      | cbr:vaults:update         | -                                                                                                                   |
| PUT /v3/<br>{project_id}/vaults/<br>batch-update                                    | cbr:vaults:update         | -                                                                                                                   |

| API                                                      | Action                        | Dependencies                                                                                                        |
|----------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------|
| DELETE /v3/{project_id}/vaults/{vault_id}                | cbr:vaults:delete             | -                                                                                                                   |
| POST /v3/{project_id}/vaults/{vault_id}/removeresources  | cbr:vaults:removeResources    | -                                                                                                                   |
| POST /v3/{project_id}/vaults/{vault_id}/addresources     | cbr:vaults:addResources       | <ul style="list-style-type: none"> <li>• ecs:cloudServers:listServersDetails</li> <li>• evs:volumes:list</li> </ul> |
| PUT /v3/{project_id}/vaults/{vault_id}/set-resources     | cbr:vaults:setResources       | -                                                                                                                   |
| POST /v3/{project_id}/vaults/{vault_id}/associatepolicy  | cbr:vaults:associatePolicy    | -                                                                                                                   |
| POST /v3/{project_id}/vaults/{vault_id}/dissociatepolicy | cbr:vaults:dissociatePolicy   | -                                                                                                                   |
| GET /v3/{project_id}/vaults/external                     | cbr:vaults:listExternalVaults | -                                                                                                                   |
| POST /v3/{project_id}/vaults/{vault_id}/migrateresources | cbr:vaults:migrateResources   | -                                                                                                                   |
| POST /v3/{project_id}/backups/sync                       | cbr:backups:sync              | -                                                                                                                   |
| GET /v3/{project_id}/backups/{backup_id}                 | cbr:backups:get               | -                                                                                                                   |
| GET /v3/{project_id}/backups/{backup_id}/metadata        | cbr:backups:showMetadata      | -                                                                                                                   |

| API                                                                          | Action                      | Dependencies                                                                                                    |
|------------------------------------------------------------------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| GET /v3/{project_id}/backups                                                 | cbr:backups:list            | -                                                                                                               |
| DELETE /v3/{project_id}/backups/{backup_id}                                  | cbr:backups:delete          | -                                                                                                               |
| POST /v3/{project_id}/backups/{backup_id}/replicate                          | cbr:backups:replicate       | -                                                                                                               |
| POST /v3/{project_id}/backups/{backup_id}/restore                            | cbr:backups:restore         | <ul style="list-style-type: none"> <li>ecs:cloudServers:listServersDetails</li> <li>evs:volumes:list</li> </ul> |
| PUT /v3/{project_id}/backups/{backup_id}                                     | cbr:backups:update          | -                                                                                                               |
| GET /v3/{project_id}/policies                                                | cbr:policies:list           | -                                                                                                               |
| POST /v3/{project_id}/policies                                               | cbr:policies:create         | -                                                                                                               |
| GET /v3/{project_id}/policies/{policy_id}                                    | cbr:policies:get            | -                                                                                                               |
| PUT /v3/{project_id}/policies/{policy_id}                                    | cbr:policies:update         | -                                                                                                               |
| DELETE /v3/{project_id}/policies/{policy_id}                                 | cbr:policies:delete         | -                                                                                                               |
| GET /v3/{project_id}/protectables/{protectable_type}/instances               | cbr:vaults:listProtectables | <ul style="list-style-type: none"> <li>ecs:cloudServers:listServersDetails</li> <li>evs:volumes:list</li> </ul> |
| GET /v3/{project_id}/protectables/{protectable_type}/instances/{instance_id} | cbr:vaults:getProtectables  | <ul style="list-style-type: none"> <li>ecs:cloudServers:listServersDetails</li> <li>evs:volumes:list</li> </ul> |

| API                                                   | Action                                 | Dependencies |
|-------------------------------------------------------|----------------------------------------|--------------|
| GET /v3/{project_id}/replication-capabilities         | cbr:backups:queryReplicationCapability | -            |
| POST /v3/{project_id}/agent/check                     | cbr:backups:checkAgent                 | -            |
| POST /v3/{project_id}/vault/resource_instances/action | cbr:vaults:listResourceInstances       | -            |
| POST /v3/{project_id}/vault/{vault_id}/tags/action    | cbr:vaults:bulkCreateOrDeleteTags      | -            |
| POST /v3/{project_id}/vault/{vault_id}/tags           | cbr:vaults:setTags                     | -            |
| DELETE /v3/{project_id}/vault/{vault_id}/tags/{key}   | cbr:vaults:deleteTags                  | -            |
| GET /v3/{project_id}/vault/{vault_id}/tags            | cbr:vaults:getTags                     | -            |
| GET /v3/{project_id}/vault/tags                       | cbr:vaults:listProjectTags             | -            |
| GET /v3/{project_id}/storage_usage                    | cbr:backups:listStorageUsage           | -            |
| PUT /v3/{project_id}/orders/{order_id}                | cbr:vaults:updateOrder                 | -            |
| POST /v3/{project_id}/agents/{agent_id}/add-path      | cbr:agents:addPath                     | -            |
| GET /v3/{project_id}/agents/{agent_id}                | cbr:agents:get                         | -            |

| API                                                                               | Action                                    | Dependencies |
|-----------------------------------------------------------------------------------|-------------------------------------------|--------------|
| PUT /v3/{project_id}/agents/{agent_id}                                            | cbr:agents:update                         | -            |
| POST /v3/{project_id}/agents                                                      | cbr:agents:register                       | -            |
| DELETE /v3/{project_id}/agents/{agent_id}                                         | cbr:agents:delete                         | -            |
| POST /v3/{project_id}/agents/{agent_id}/remove-path                               | cbr:agents:removePath                     | -            |
| GET /v3/{project_id}/agents                                                       | cbr:agents:list                           | -            |
| POST /v3/migrates                                                                 | cbr:backups:migratesCreate                | -            |
| GET /v3/migrates                                                                  | cbr:backups:migratesIndex                 | -            |
| POST /v3/{project_id}/organization-policies                                       | cbr:organizationPolicies:create           | -            |
| GET /v3/{project_id}/organization-policies/{organization_policy_id}/policy-detail | cbr:organizationPolicies:listPolicyDetail | -            |
| DELETE /v3/{project_id}/organization-policies/{organization_policy_id}            | cbr:organizationPolicies:delete           | -            |
| PUT /v3/{project_id}/organization-policies/{organization_policy_id}               | cbr:organizationPolicies:update           | -            |
| GET /v3/{project_id}/organization-policies                                        | cbr:organizationPolicies:list             | -            |

| API                                                                 | Action                       | Dependencies |
|---------------------------------------------------------------------|------------------------------|--------------|
| GET /v3/{project_id}/organization-policies/{organization_policy_id} | cbr:organizationPolicies:get | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-30](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CBR.

**Table 3-30** Resource types supported by CBR

| Resource Type | URN                                                 |
|---------------|-----------------------------------------------------|
| vault         | cbr:<region>:<account-id>:vault:<vault-id>          |
| policy        | cbr:<region>:<account-id>:policy:<policy-id>        |
| rackGroup     | cbr:<region>:<account-id>:rackGroup:<rack-group-id> |
| task          | cbr:<region>:<account-id>:task:<task-id>            |
| backup        | cbr:<region>:<account-id>:backup:<backup-id>        |
| agent         | cbr:<region>:<account-id>:agent:<agent-id>          |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).



- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, cbr) apply only to operations of the xx service. For details, see [Table 3-31](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by CBR

The following table lists the condition keys that you can define in identity policies for CBR. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-31** Service-specific condition keys supported by CBR

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                           |
|--------------------------------|---------|-------------------------------|-----------------------------------------------------------------------|
| cbr:TargetOrgPaths             | string  | Single-valued                 | Filters access destination project's organization path of add member. |
| cbr:VaultId                    | string  | Single-valued                 | Filters access based on the vault ID in the request.                  |
| cbr:PolicyId                   | string  | Single-valued                 | Filters access based on the policy ID in the request.                 |
| cbr:EnabledPolicy              | boolean | Single-valued                 | Filters access by whether the policy is enabled.                      |

## 3.2.3 Elastic Volume Service (EVS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by EVS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by EVS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for identity policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for EVS.

**Table 3-32** Actions supported by EVS

| Action                          | Description                                                | Access Level | Resource Type (*: required) | Condition Key                | Alias |
|---------------------------------|------------------------------------------------------------|--------------|-----------------------------|------------------------------|-------|
| evs::enableEncryptionByDefault  | Grants permission to enable default encryption.            | Write        | -                           | -                            | -     |
| evs::disableEncryptionByDefault | Grants permission to disable default encryption.           | Write        | -                           | -                            | -     |
| evs::getEncryptionByDefault     | Grants permission to query default encryption.             | Write        | -                           | -                            | -     |
| evs::modifyDefaultKmsKeyId      | Grants permission to change the default key.               | Write        | -                           | <a href="#">evs:KmsKeyId</a> | -     |
| evs::resetDefaultKmsKeyId       | Grants permission to reset the default key to evs/default. | Write        | -                           | -                            | -     |
| evs::getDefaultKmsKeyId         | Grants permission to query the default key.                | Write        | -                           | -                            | -     |
| evs:volumes:create              | Grants permission to create disks.                         | Write        | volume *                    | -                            | -     |

| Action | Description | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Alias |
|--------|-------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|        |             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">cbr:VaultId</a></li> <li>• <a href="#">evs:KmsKeyId</a></li> <li>• <a href="#">evs:ImageId</a></li> <li>• <a href="#">evs:BackupId</a></li> <li>• <a href="#">evs:SnapshotId</a></li> <li>• <a href="#">evs:AvailabilityZone</a></li> <li>• <a href="#">evs:VolumeType</a></li> <li>• <a href="#">evs:VolumeSize</a></li> <li>• <a href="#">evs:VolumeIops</a></li> <li>• <a href="#">evs:VolumeThroughput</a></li> <li>• <a href="#">evs:ChargingMode</a></li> <li>• <a href="#">evs:ServerServiceType</a></li> <li>• <a href="#">ecs:ServerId</a></li> <li>• <a href="#">bms:ServerId</a></li> </ul> |       |

| Action                | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias              |
|-----------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
|                       |                                                      |              |                             | <ul style="list-style-type: none"> <li>• <a href="#">evs:SourceAvailabilityZone</a></li> </ul>                                                     |                    |
| evs:volumes:list      | Grants permission to list disks.                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                  |
| evs:volumes:get       | Grants permission to query disks.                    | Read         | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                  |
| evs:volumes:delete    | Grants permission to delete disks.                   | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                  |
| evs:volumes:update    | Grants permission to update disks.                   | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                  |
| evs:volumes:resize    | Grants permission to expand disk capacities.         | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | evs:volumes:extend |
| evs:volumes:modifyQos | Grants permission to modify disk QoS configurations. | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | evs:volumes:extend |

| Action                       | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| evs:volumes:resettype        | Grants permission to change disk types.                  | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| evs:volumes:revert           | Grants permission to recover disks from the recycle bin. | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| evs:recycle_policy:get       | Grants permission to query the recycle bin policy.       | Read         | -                           | -                                                                                                                                                  | -     |
| evs:recycle_policy:update    | Grants permission to update the recycle bin policy.      | Write        | -                           | -                                                                                                                                                  | -     |
| evs:volumes:changeChargeMode | Grants permission to change the disk billing mode.       | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| evs:snapshots:create         | Grants permission to create snapshots for disks.         | Write        | snapshot *                  | -                                                                                                                                                  | -     |
|                              |                                                          |              | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |       |

| Action                  | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|-------------------------|-----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                         |                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">evs:SourceAvailabilityZone</a></li> <li>• <a href="#">evs:AvailabilityZone</a></li> </ul>     |                       |
| evs:snapshots:list      | Grants permission to list snapshots.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                     |
| evs:snapshots:get       | Grants permission to query snapshots.               | Read         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                     |
| evs:snapshots:delete    | Grants permission to delete snapshots.              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                     |
| evs:snapshots:update    | Grants permission to update snapshots.              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                     |
| evs:snapshots:rollback  | Grants permission to roll back data from snapshots. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                     |
| evs:types:get           | Grants permission to query disk types.              | Read         | -                           | -                                                                                                                                                  | -                     |
| evs:quotas:get          | Grants permission to query EVS quotas.              | Read         | -                           | -                                                                                                                                                  | -                     |
| evs:volumes:tagResource | Grants permission to add tags to a disk.            | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | evs:volumeTags:create |

| Action                          | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                  |
|---------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|                                 |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                        |
| evs:volumes:unTagResource       | Grants permission to delete tags from a disk.              | Write        | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | evs:volumeTags:delete  |
|                                 |                                                            |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |                        |
| evs:volumes:listTags            | Grants permission to query all disk tags in a project.     | List         | -                           | -                                                                                                                                                  | evs:volumeTags:list    |
| evs:volumes:listTagsForResource | Grants permission to query disk tags.                      | Read         | volume *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | evs:volumeTags:getById |
| evs:volumes:listResourcesByTag  | Grants permission to list disks by tag.                    | List         | -                           | <a href="#">g:TagKeys</a>                                                                                                                          | evs:volumeTags:get     |
| evs:volumes:use                 | Grants permission to allow ECSs and BMSs to use EVS disks. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                      |

Each API of EVS usually supports one or more actions. [Table 3-33](#) lists the supported actions and dependencies.



**Table 3-33** Actions and dependencies supported by EVS APIs

| API                                               | Action                          | Dependencies      |
|---------------------------------------------------|---------------------------------|-------------------|
| POST /v5/{project_id}/default-encryption/enable   | evs::enableEncryptionByDefault  | -                 |
| POST /v5/{project_id}/default-encryption/disable  | evs::disableEncryptionByDefault | -                 |
| GET /v5/{project_id}/default-encryption/status    | evs::getEncryptionByDefault     | -                 |
| PUT /v5/{project_id}/default-encryption/key       | evs::modifyDefaultKmsKeyId      | -                 |
| PUT /v5/{project_id}/default-encryption/key/reset | evs::resetDefaultKmsKeyId       | -                 |
| GET /v5/{project_id}/default-encryption/key       | evs::getDefaultKmsKeyId         | -                 |
| POST /v2.1/{project_id}/cloudvolumes              | evs:volumes:create              | billing:order:pay |
| POST /v2/{project_id}/cloudvolumes                | evs:volumes:create              | -                 |
| POST /v3/{project_id}/cloudvolumes                | evs:volumes:create              | -                 |
| GET /v2/{project_id}/cloudvolumes/detail          | evs:volumes:list                | -                 |
| GET /v2/{project_id}/cloudvolumes/{volume_id}     | evs:volumes:get                 | -                 |
| DELETE /v2/{project_id}/cloudvolumes/{volume_id}  | evs:volumes:delete              | -                 |

| API                                                     | Action                       | Dependencies                                                                                                |
|---------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------|
| PUT /v2/{project_id}/cloudvolumes/{volume_id}           | evs:volumes:update           | -                                                                                                           |
| POST /v2.1/{project_id}/cloudvolumes/{volume_id}/action | evs:volumes:resize           | billing:order:pay                                                                                           |
| -                                                       | evs:volumes:resize           | billing:order:pay                                                                                           |
| POST /v2/{project_id}/cloudvolumes/{volume_id}/action   | evs:volumes:resize           | -                                                                                                           |
| PUT /v5/{project_id}/cloudvolumes/{volume_id}/qos       | evs:volumes:modifyQos        | -                                                                                                           |
| POST /v2/{project_id}/volumes/{volume_id}/retype        | evs:volumes:retype           | billing:order:pay                                                                                           |
| POST /v2/{project_id}/cloudvolumes/unsubscribe          | evs:volumes:delete           | billing:subscription:unsubscribe                                                                            |
| POST /v2/{project_id}/cloudvolumes/change-charge-mode   | evs:volumes:changeChargeMode | <ul style="list-style-type: none"> <li>• billing:order:pay</li> <li>• billing:subscription:renew</li> </ul> |
| POST /v2/{project_id}/cloudsnapshots                    | evs:snapshots:create         | -                                                                                                           |
| GET /v2/{project_id}/cloudsnapshots/detail              | evs:snapshots:list           | -                                                                                                           |
| GET /v2/{project_id}/cloudsnapshots/{snapshot_id}       | evs:snapshots:get            | -                                                                                                           |

| API                                                           | Action                          | Dependencies |
|---------------------------------------------------------------|---------------------------------|--------------|
| DELETE /v2/{project_id}/cloudsnapshots/{snapshot_id}          | evs:snapshots:delete            | -            |
| PUT /v2/{project_id}/cloudsnapshots/{snapshot_id}             | evs:snapshots:update            | -            |
| POST /v2/{project_id}/cloudsnapshots/{snapshot_id}/rollback   | evs:snapshots:rollback          | -            |
| POST /v2/{project_id}/cloudvolumes/{volume_id}/tags/action    | evs:volumes:tagResource         | -            |
| POST 01 /v2/{project_id}/cloudvolumes/{volume_id}/tags/action | evs:volumes:unTagResource       | -            |
| GET /v2/{project_id}/cloudvolumes/tags                        | evs:volumes:listTags            | -            |
| GET /v2/{project_id}/cloudvolumes/{volume_id}/tags            | evs:volumes:listTagsForResource | -            |
| POST /v2/{project_id}/cloudvolumes/resource_instances/action  | evs:volumes:listResourcesByTag  | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-34](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for EVS.

**Table 3-34** Resource types supported by EVS

| Resource Type | URN                                                  |
|---------------|------------------------------------------------------|
| imageCache    | evs:<region>:<account-id>:imageCache:<imageCache-id> |
| snapshot      | evs:<region>:<account-id>:snapshot:<snapshot-id>     |
| volume        | evs:<region>:<account-id>:volume:<volume-id>         |

## Conditions

### About condition keys

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, evs:) apply only to operations of EVS. For details, see [Table 3-35](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by EVS

The following table lists the condition keys that you can define in custom identity policies for EVS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-35** Service-specific condition keys supported by EVS

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                   |
|--------------------------------|---------|-------------------------------|---------------------------------------------------------------|
| evs:KmsKeyId                   | string  | Single-valued                 | Filters access based on the key ID used by the disk.          |
| evs:Encrypted                  | boolean | Single-valued                 | Filters access based on whether the disk is encrypted.        |
| evs:KmsKeyId                   | string  | Single-valued                 | Filters access based on the key ID used by the disk.          |
| evs:ImageId                    | string  | Single-valued                 | Filters access by image ID.                                   |
| evs:BackupId                   | string  | Single-valued                 | Filters access by backup ID.                                  |
| evs:SnapshotId                 | string  | Single-valued                 | Filters access by snapshot ID.                                |
| evs:AvailabilityZone           | string  | Single-valued                 | Filters access based on the AZ of the disk.                   |
| evs:SourceAvailability-Zone    | string  | Single-valued                 | Filters access by source AZ.                                  |
| evs:VolumeType                 | string  | Single-valued                 | Filters access by disk type.                                  |
| evs:VolumeSize                 | numeric | Single-valued                 | Filters access by disk capacity.                              |
| evs:Volumelops                 | numeric | Single-valued                 | Filters access by disk IOPS.                                  |
| evs:VolumeThroughput           | numeric | Single-valued                 | Filters access by disk throughput.                            |
| evs:ChargingMode               | string  | Single-valued                 | Filters access by disk billing mode.                          |
| evs:ServerServiceType          | string  | Single-valued                 | Filters access based on the service type of the cloud server. |
| evs:Volumeld                   | string  | Single-valued                 | Filters access by disk ID.                                    |

### 3.2.4 Scalable File Service Turbo (SFS Turbo)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by SFS Turbo, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.

- If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by SFS Turbo, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for identity policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for SFS Turbo.

**Table 3-36** Actions supported by SFS Turbo

| Action                       | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                | Alias |
|------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:createShare  | Grants permission to create SFS Turbo file systems.               | write        | shares *                    | <ul style="list-style-type: none"> <li>• g:EnterpriseProjectId</li> <li>• g:TagKeys</li> <li>• g:RequestTag/&lt;tag-key&gt;</li> <li>• sfsturbo:CryptKeyId</li> <li>• cbr:VaultId</li> </ul> | -     |
| sfsturbo:shares:deleteShare  | Grants permission to delete SFS Turbo file systems.               | write        | shares *                    | <ul style="list-style-type: none"> <li>• g:ResourceTag/&lt;tag-key&gt;</li> <li>• g:EnterpriseProjectId</li> </ul>                                                                           | -     |
| sfsturbo:shares:getAllShares | Grants permission to list SFS Turbo file systems.                 | list         | -                           | <ul style="list-style-type: none"> <li>• g:EnterpriseProjectId</li> <li>• g:RequestTag/&lt;tag-key&gt;</li> <li>• g:TagKeys</li> </ul>                                                       | -     |
| sfsturbo:shares:getShare     | Grants permission to query SFS Turbo file systems.                | read         | shares *                    | <ul style="list-style-type: none"> <li>• g:ResourceTag/&lt;tag-key&gt;</li> <li>• g:EnterpriseProjectId</li> </ul>                                                                           | -     |
| sfsturbo:shares:extendShare  | Grants permission to expand capacities of SFS Turbo file systems. | write        | shares *                    | <ul style="list-style-type: none"> <li>• g:ResourceTag/&lt;tag-key&gt;</li> <li>• g:EnterpriseProjectId</li> </ul>                                                                           | -     |

| Action                                   | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:updateHpcShare           | Grants permission to update SFS Turbo file systems.                        | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:updateShareSecurityGroup | Grants permission to change the security groups of SFS Turbo file systems. | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:addTag                   | Grants permission to add a tag to an SFS Turbo file system.                | tagging      | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>             | -     |
| sfsturbo:shares:getTag                   | Grants permission to query tags of an SFS Turbo file system.               | read         | shares *                    | g:EnterpriseProjectId                                                                                          | -     |
| sfsturbo:shares:deleteTag                | Grants permission to delete tags from an SFS Turbo file system.            | tagging      | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>             | -     |
| sfsturbo:shares:batchResTag              | Grants permission to batch add tags to an SFS Turbo file system.           | tagging      | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>             | -     |
| sfsturbo:shares:getAllTag                | Grants permission to list all tags of an SFS Turbo file system.            | list         | -                           | g:EnterpriseProjectId                                                                                          | -     |



| Action                                    | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|-------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:renameShare               | Grants permission to change SFS Turbo file system names.                        | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showClientInfo            | Grants permission to query the client IP addresses of an SFS Turbo file system. | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:createDataRepositoryTask  | Grants permission to create SFS Turbo backup vaults.                            | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:deleteDataRepositoryTask  | Grants permission to delete SFS Turbo backup vaults.                            | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:getDataRepositoryTask     | Grants permission to query SFS Turbo backup vaults.                             | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:getAllDataRepositoryTasks | Grants permission to list SFS Turbo backup vaults.                              | list         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:getAZInfo                 | Grants permission to query the AZ information of the current region.            | read         | -                           | -                                                                                                              | -     |
| sfsturbo:shares:getQuota                  | Grants permission to query SFS Turbo quotas.                                    | read         | -                           | -                                                                                                              | -     |

| Action                           | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|----------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:getFlavors       | Grants permission to query SFS Turbo file system types.                                | read         | -                           | -                                                                                                              | -     |
| sfsturbo:shares:checkShareName   | Grants permission to check SFS Turbo file system names.                                | read         | -                           | -                                                                                                              | -     |
| sfsturbo:shares:createFsDir      | Grants permission to create directories in SFS Turbo file systems.                     | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showFsDir        | Grants permission to query directories of SFS Turbo file systems.                      | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:deleteFsDir      | Grants permission to delete directories from SFS Turbo file systems.                   | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:createFsDirQuota | Grants permission to configure quota limits for directories in SFS Turbo file systems. | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showFsDirQuota   | Grants permission to query quota limits of directories in SFS Turbo file systems.      | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |

| Action                                 | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|----------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:deleteFsDirQuota       | Grants permission to remove quota limits from directories in SFS Turbo file systems.         | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:updateFsDirQuota       | Grants permission to update quota limits of directories in SFS Turbo file systems.           | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:batchCreateFsDirQuotas | Grants permission to batch configure quota limits for directories in SFS Turbo file systems. | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:listFsDirQuotas        | Grants permission to list quota limits of directories in SFS Turbo file systems.             | list         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showFsDirUsage         | Grants permission to query usages of directories in SFS Turbo file systems.                  | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:createFsAsyncTask      | Grants permission to create asynchronous tasks of SFS Turbo file systems.                    | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |

| Action                                | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|---------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:showFsAsyncTask       | Grants permission to query details of asynchronous tasks of SFS Turbo file systems.  | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:listFsAsyncTasks      | Grants permission to list asynchronous tasks of SFS Turbo file systems.              | list         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:deleteFsAsyncTask     | Grants permission to delete asynchronous tasks of SFS Turbo file systems.            | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:createBackendTarget   | Grants permission to add storage backends of SFS Turbo file systems.                 | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showBackendTargetInfo | Grants permission to query details about storage backends of SFS Turbo file systems. | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:listBackendTargets    | Grants permission to list storage backends of SFS Turbo file systems.                | list         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |

| Action                                    | Description                                                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:deleteBackendTarget       | Grants permission to remove storage backends of SFS Turbo file systems.                                              | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:updateObsTargetPolicy     | Grants permission to modify the auto synchronization policy between SFS Turbo file systems and OBS storage backends. | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:updateObsTargetAttributes | Grants permission to modify attributes of storage backends of SFS Turbo file systems.                                | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:listPermRules             | Grants permission to list permission rules of SFS Turbo file systems.                                                | list         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showPermRule              | Grants permission to query details of permissions rules of SFS Turbo file systems.                                   | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |

| Action                         | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|--------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:createPermRule | Grants permission to create permissions rules of SFS Turbo file systems.      | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:updatePermRule | Grants permission to modify permissions rules of SFS Turbo file systems.      | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:deletePermRule | Grants permission to delete permissions rules of SFS Turbo file systems.      | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showLdap       | Grants permission to query the LDAP configuration of SFS Turbo file systems.  | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:createLdap     | Grants permission to create the LDAP configuration of SFS Turbo file systems. | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:updateLdap     | Grants permission to modify the LDAP configuration of SFS Turbo file systems. | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |

| Action                                      | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|---------------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| sfsturbo:shares:deleteLdap                  | Grants permission to delete the LDAP configuration of SFS Turbo file systems.        | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:addActiveDirectoryDomain    | Grants permission to add SFS Turbo file systems to AD domains.                       | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:deleteActiveDirectoryDomain | Grants permission to remove SFS Turbo file systems from AD domains.                  | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:showActiveDirectoryDomain   | Grants permission to query AD domains of SFS Turbo file systems.                     | read         | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:updateActiveDirectoryDomain | Grants permission to modify the AD domain configuration of an SFS Turbo file system. | write        | shares *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| sfsturbo:shares:getJob                      | Grants permission to query details of tasks in SFS Turbo file systems.               | read         | -                           | -                                                                                                              | -     |

Each API of SFS Turbo usually supports one or more actions. [Table 3-37](#) lists the actions and dependencies supported by SFS Turbo APIs.

**Table 3-37** Actions and dependencies supported by SFS Turbo APIs

| API                                                 | Action                       | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/{project_id}/sfs-turbo/shares              | sfsturbo:shares:createShare  | <ul style="list-style-type: none"> <li>• billing:order:pay</li> <li>• billing:contract:viewDiscount</li> <li>• vpc:vpcs:get</li> <li>• vpc:subnets:get</li> <li>• vpc:securityGroups:get</li> <li>• vpc:securityGroups:create</li> <li>• vpc:ports:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> <li>• vpc:securityGroupRules:get</li> <li>• vpc:securityGroupRules:create</li> <li>• vpc:quotas:list</li> <li>• cbr:backups:get</li> <li>• cbr:vaults:addResources</li> <li>• evs:types:get</li> <li>• kms:cmk:listGrants</li> <li>• kms:cmk:createGrant</li> <li>• kms:cmk:get</li> <li>• sfsturbo:shares:getAZInfo</li> <li>• sfsturbo:shares:getQuota</li> <li>• sfsturbo:shares:getFlavors</li> <li>• sfsturbo:shares:checkShareName</li> <li>• eps:enterpriseProjects:list</li> </ul> |
| GET /v1/{project_id}/sfs-turbo/shares/detail        | sfsturbo:shares:getAllShares | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}    | sfsturbo:shares:getShare     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id} | sfsturbo:shares:deleteShare  | <ul style="list-style-type: none"> <li>• vpc:ports:get</li> <li>• vpc:ports:delete</li> <li>• vpc:securityGroupRules:delete</li> <li>• vpc:securityGroups:delete</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



| API                                                                  | Action                                   | Dependencies                                                                                                                                                                                              |
|----------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action             | sfsturbo:shares:extendShare              | <ul style="list-style-type: none"> <li>• billing:order:pay</li> <li>• vpc:vpcs:get</li> <li>• vpc:subnets:get</li> <li>• vpc:ports:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> </ul> |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action             | sfsturbo:shares:updateShareSecurityGroup | <ul style="list-style-type: none"> <li>• vpc:ports:update</li> <li>• vpc:securityGroups:get</li> <li>• vpc:securityGroupRules:create</li> <li>• vpc:securityGroupRules:delete</li> </ul>                  |
| POST /v1/{project_id}/sfs-turbo/{share_id}/tags                      | sfsturbo:shares:addTag                   | -                                                                                                                                                                                                         |
| GET /v1/{project_id}/sfs-turbo/{share_id}/tags                       | sfsturbo:shares:getTag                   | -                                                                                                                                                                                                         |
| DELETE /v1/{project_id}/sfs-turbo/{share_id}/tags/{key}              | sfsturbo:shares:deleteTag                | -                                                                                                                                                                                                         |
| POST /v1/{project_id}/sfs-turbo/{share_id}/tags/action               | sfsturbo:shares:batchResTag              | -                                                                                                                                                                                                         |
| POST /v1/{project_id}/sfs-turbo/resource_instances/action            | sfsturbo:shares:getAllTag                | -                                                                                                                                                                                                         |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action             | sfsturbo:shares:renameShare              | -                                                                                                                                                                                                         |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks | sfsturbo:shares:createFsAsyncTask        | -                                                                                                                                                                                                         |

| API                                                                              | Action                                   | Dependencies                                                                                                                                           |
|----------------------------------------------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks              | sfsturbo:shares:listFsAsyncTasks         | -                                                                                                                                                      |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks/{task_id}    | sfsturbo:shares:showFsAsyncTask          | -                                                                                                                                                      |
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/{feature}/tasks/{task_id} | sfsturbo:shares:deleteFsAsyncTask        | -                                                                                                                                                      |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/targets                        | sfsturbo:shares:createBackendTarget      | <ul style="list-style-type: none"> <li>obs:bucket:putBucketPolicy</li> <li>vpc:ports:get</li> <li>vpc:ports:create</li> <li>vpc:subnets:get</li> </ul> |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/targets                         | sfsturbo:shares:listBackendTargets       | -                                                                                                                                                      |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}             | sfsturbo:shares:showBackendTargetInfo    | -                                                                                                                                                      |
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}          | sfsturbo:shares:deleteBackendTarget      | -                                                                                                                                                      |
| POST /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task                        | sfsturbo:shares:createDataRepositoryTask | obs:bucket:headBucket                                                                                                                                  |
| GET /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task/{task_id}               | sfsturbo:shares:getDataRepositoryTask    | -                                                                                                                                                      |

| API                                                              | Action                                    | Dependencies |
|------------------------------------------------------------------|-------------------------------------------|--------------|
| GET /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/tasks        | sfsturbo:shares:getAllDataRepositoryTasks | -            |
| PUT /v1/{project_id}/sfs-turbo/shares/{share_id}                 | sfsturbo:shares:updateHpcShare            | -            |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota   | sfsturbo:shares:createFsDirQuota          | -            |
| PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota    | sfsturbo:shares:updateFsDirQuota          | -            |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota    | sfsturbo:shares:showFsDirQuota            | -            |
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-quota | sfsturbo:shares:deleteFsDirQuota          | -            |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir         | sfsturbo:shares:createFsDir               | -            |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir          | sfsturbo:shares:showFsDir                 | -            |
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir       | sfsturbo:shares:deleteFsDir               | -            |

| API                                                                         | Action                             | Dependencies |
|-----------------------------------------------------------------------------|------------------------------------|--------------|
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-usage               | sfsturbo:shares:s<br>howFsDirUsage | -            |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules             | sfsturbo:shares:c<br>reatePermRule | -            |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules              | sfsturbo:shares:li<br>stPermRules  | -            |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}    | sfsturbo:shares:s<br>howPermRule   | -            |
| PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}    | sfsturbo:shares:u<br>pdatePermRule | -            |
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id} | sfsturbo:shares:d<br>eletePermRule | -            |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap                   | sfsturbo:shares:c<br>reateLdap     | -            |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap                    | sfsturbo:shares:s<br>howLdap       | -            |
| PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap                    | sfsturbo:shares:u<br>pdateLdap     | -            |

| API                                                                             | Action                                      | Dependencies |
|---------------------------------------------------------------------------------|---------------------------------------------|--------------|
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap                     | sfsturbo:shares:deleteLdap                  | -            |
| GET /v1/{project_id}/sfs-turbo/jobs/{job_id}                                    | sfsturbo:shares:getJob                      | -            |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action                        | sfsturbo:shares:showClientIpInfo            | -            |
| DELETE /v1/{project_id}/sfs-turbo/{share_id}/hpc-cache/task/{task_id}           | sfsturbo:shares:deleteDataRepositoryTask    | -            |
| PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}/policy     | sfsturbo:shares:updateObsTargetPolicy       | -            |
| PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/targets/{target_id}/attributes | sfsturbo:shares:updateObsTargetAttributes   | -            |
| POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain    | sfsturbo:shares:addActiveDirectoryDomain    | -            |
| DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain  | sfsturbo:shares:deleteActiveDirectoryDomain | -            |
| GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain     | sfsturbo:shares:showActiveDirectoryDomain   | -            |

| API                                                                         | Action                                      | Dependencies |
|-----------------------------------------------------------------------------|---------------------------------------------|--------------|
| PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/active-directory-domain | sfsturbo:shares:updateActiveDirectoryDomain | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-38](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for SFS Turbo.

**Table 3-38** Resource types supported by SFS Turbo

| Resource Type | URN      |
|---------------|----------|
| shares        | shares * |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name as the prefix, for example, sfsturbo) apply only to operations of SFS Turbo. For details, see [Table 3-39](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple

tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.

- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by SFS Turbo

The following table lists the condition keys that you can define in identity policies for SFS Turbo. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-39** Service-specific condition keys supported by SFS Turbo

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                            |
|--------------------------------|--------|-------------------------------|------------------------------------------------------------------------|
| sfsturbo:CryptKeyId            | String | Single-valued                 | Filters access based on the key ID specified in the request parameter. |

## 3.3 Networking

### 3.3.1 Enterprise Router

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by er, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by er, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for er.

**Table 3-40** Actions supported by er

| Action           | Description                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------|------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| er:instances:get | Grants permission to get an enterprise router. | Read         | instances *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |



| Action                           | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                | Alias                 |
|----------------------------------|-------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| er:instances:create              | Grants permission to create an enterprise router.           | Write        | instances *                 | <b>g:EnterpriseProjectId</b>                                                                                                 | -                     |
|                                  |                                                             |              | -                           | <ul style="list-style-type: none"> <li><b>g:RequestTag/&lt;tag-key&gt;</b></li> <li><b>g:TagKeys</b></li> </ul>              |                       |
| er:instances:list                | Grants permission to list enterprise routers.               | List         | instances *                 | -                                                                                                                            | -                     |
| er:instances:update              | Grants permission to update an enterprise router.           | Write        | instances *                 | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul> | -                     |
| er:instances:delete              | Grants permission to delete an enterprise router.           | Write        | instances *                 | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul> | -                     |
| er:instances:changeAZ            | Grants permission to change the AZ of an enterprise router. | Write        | instances *                 | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul> | -                     |
| er:instances:createVpcAttachment | Grants permission to create a VPC attachment.               | Write        | instances *                 | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul> | er:attachments:create |

| Action                           | Description                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|----------------------------------|-----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| er:instances:showVpcAttachment   | Grants permission to get a VPC attachment.    | Read         | instances *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:attachments:get    |
| er:instances:listVpcAttachments  | Grants permission to list VPC attachments.    | List         | instances *                 | -                                                                                                                                                  | er:attachments:list   |
| er:instances:updateVpcAttachment | Grants permission to update a VPC attachment. | Write        | instances *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:attachments:update |
| er:instances:deleteVpcAttachment | Grants permission to delete a VPC attachment. | Write        | instances *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:attachments:delete |
| er:commonAttachments:get         | Grants permission to get an attachment.       | Read         | attachments *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:attachments:get    |
| er:commonAttachments:list        | Grants permission to list attachments.        | List         | attachments *               | -                                                                                                                                                  | er:attachments:list   |
| er:commonAttachments:update      | Grants permission to update an attachment.    | Write        | attachments *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:attachments:update |

| Action                | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias |
|-----------------------|--------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| er:attachments:accept | Grants permission to accept an attachment. | Write        | attachments *               | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -     |
| er:attachments:reject | Grants permission to reject an attachment. | Write        | attachments *               | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -     |
| er:routeTables:get    | Grants permission to get a route table.    | Read         | routeTables *               | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| er:routeTables:create | Grants permission to create a route table. | Write        | routeTables *               | -                                                                                                                                              | -     |
|                       |                                            |              | instances *                 | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                       |                                            |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              |       |
| er:routeTables:list   | Grants permission to list route tables.    | List         | routeTables *               | -                                                                                                                                              | -     |
| er:routeTables:update | Grants permission to update a route table. | Write        | routeTables *               | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

| Action                          | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                        |
|---------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| er:routeTables:delete           | Grants permission to delete a route table.                          | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                            |
| er:routeTables:associate        | Grants permission to associate an attachment with a route table.    | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:associations:associate    |
|                                 |                                                                     |              | attachments *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                              |
| er:routeTables:disassociate     | Grants permission to disassociate an attachment with a route table. | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:associations:disassociate |
|                                 |                                                                     |              | attachments *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                              |
| er:routeTables:listAssociations | Grants permission to list associations.                             | List         | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:associations:list         |

| Action                            | Description                                                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| er:routeTables:enablePropagation  | Grants permission to enable an attachment to propagate routes to a propagation route table.                          | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:propagations:enable  |
|                                   |                                                                                                                      |              | attachments *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                         |
| er:routeTables:disablePropagation | Grants permission to disable a resource attachment from propagating routes to the specified propagation route table. | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:propagations:disable |
|                                   |                                                                                                                      |              | attachments *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                         |
| er:routeTables:listPropagations   | Grants permission to list propagations.                                                                              | List         | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:propagations:list    |
| er:staticRoutes:list              | Grants permission to list static routes.                                                                             | List         | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:routes:list          |

| Action                  | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias            |
|-------------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| er:staticRoutes:create  | Grants permission to create a static route. | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:routes:create |
|                         |                                             |              | attachments                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                  |
| er:effectiveRoutes:list | Grants permission to list effective routes. | List         | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:routes:list   |
| er:staticRoutes:delete  | Grants permission to delete a static route. | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:routes:delete |
| er:staticRoutes:update  | Grants permission to update a static route. | Write        | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:routes:update |
|                         |                                             |              | attachments                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                  |

| Action               | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias          |
|----------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| er:staticRoutes:get  | Grants permission to get a static route.    | Read         | route Tables *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:routes:get  |
| er:tags:singleCreate | Grants permission to create a resource tag. | Write        | route Tables                | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:tags:create |
|                      |                                             |              | instances                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                |
|                      |                                             |              | attachments                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                |
| er:tags:delete       | Grants permission to delete a resource tag. | Write        | route Tables                | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -              |
|                      |                                             |              | instances                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                |

| Action                  | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias          |
|-------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                         |                                                            |              | attachments                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                |
| er:tags:batch Operation | Grants permission to batch create or delete resource tags. | Write        | route Tables                | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | er:tags:create |
|                         |                                                            |              | instances                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                |
|                         |                                                            |              | attachments                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                |
| er:tags:get             | Grants permission to get the tags of a resource.           | Read         | route Tables                | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -              |
|                         |                                                            |              | instances                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                |



| Action             | Description                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------|------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                    |                                          |              | attachments                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
| er:tags:list       | Grants permission to list resource tags. | List         | -                           | -                                                                                                                                                  | -     |
| er:quotas:list     | Grants permission to list quotas.        | List         | -                           | -                                                                                                                                                  | -     |
| er:flowLogs:create | Grants permission to create flow log.    | Write        | instances *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                    |                                          |              | attachments *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                    |                                          |              | flowLogs *                  | -                                                                                                                                                  |       |
| er:flowLogs:list   | Grants permission to list flow log.      | List         | flowLogs *                  | -                                                                                                                                                  | -     |
| er:flowLogs:get    | Grants permission to show flow log.      | Read         | flowLogs *                  | -                                                                                                                                                  | -     |
| er:flowLogs:update | Grants permission to update flow log.    | Write        | flowLogs *                  | -                                                                                                                                                  | -     |

| Action              | Description                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------|----------------------------------------|--------------|-----------------------------|---------------|-------|
| er:flowLogs:delete  | Grants permission to delete flow log.  | Write        | flowLogs *                  | -             | -     |
| er:flowLogs:enable  | Grants permission to enable flow log.  | Write        | flowLogs *                  | -             | -     |
| er:flowLogs:disable | Grants permission to disable flow log. | Write        | flowLogs *                  | -             | -     |

Each API of er usually supports one or more actions. [Table 3-41](#) lists the supported actions and dependencies.

**Table 3-41** Actions and dependencies supported by er APIs

| API                                                                                    | Action                           | Dependencies |
|----------------------------------------------------------------------------------------|----------------------------------|--------------|
| POST /v3/{project_id}/enterprise-router/instances                                      | er:instances:create              | -            |
| PUT /v3/{project_id}/enterprise-router/instances/{er_id}                               | er:instances:update              | -            |
| GET /v3/{project_id}/enterprise-router/instances/{er_id}                               | er:instances:get                 | -            |
| GET /v3/{project_id}/enterprise-router/instances                                       | er:instances:list                | -            |
| POST /v3/{project_id}/enterprise-router/instances/{er_id}/change-availability-zone-ids | er:instances:changeAZ            | -            |
| DELETE /v3/{project_id}/enterprise-router/instances/{er_id}                            | er:instances:delete              | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments                        | er:instances:createVpcAttachment | -            |
| PUT /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}     | er:instances:updateVpcAttachment | -            |

| API                                                                                               | Action                            | Dependencies |
|---------------------------------------------------------------------------------------------------|-----------------------------------|--------------|
| GET /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}                | er:instances:show VpcAttachment   | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments                                    | er:instances:listVpcAttachments   | -            |
| DELETE /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}             | er:instances:delete VpcAttachment | -            |
| PUT /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}                        | er:commonAttachments:update       | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}                        | er:commonAttachments:get          | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/attachments                                        | er:commonAttachments:list         | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}/accept                | er:attachments:accept             | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/attachments/{attachment_id}/reject                | er:attachments:reject             | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/route-tables                                      | er:routeTables:create             | -            |
| PUT /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}                      | er:routeTables:update             | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}                      | er:routeTables:get                | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/route-tables                                       | er:routeTables:list               | -            |
| DELETE /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}                   | er:routeTables:delete             | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/associate           | er:routeTables:associate          | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/associations         | er:routeTables:listAssociations   | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/disassociate        | er:routeTables:disassociate       | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/enable-propagations | er:routeTables:enablePropagation  | -            |

| API                                                                                                | Action                              | Dependencies |
|----------------------------------------------------------------------------------------------------|-------------------------------------|--------------|
| GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/propagations          | er:routeTables:list<br>Propagations | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/disable-propagations | er:routeTables:disablePropagation   | -            |
| POST /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes                | er:staticRoutes:create              | -            |
| PUT /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}      | er:staticRoutes:update              | -            |
| GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}      | er:staticRoutes:get                 | -            |
| GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes                 | er:staticRoutes:list                | -            |
| GET /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/routes                        | er:effectiveRoutes:list             | -            |
| DELETE /v3/{project_id}/enterprise-router/route-tables/{route_table_id}/static-routes/{route_id}   | er:staticRoutes:delete              | -            |
| GET /v3/{project_id}/{resource_type}/tags                                                          | er:tags:list                        | -            |
| GET /v3/{project_id}/{resource_type}/{resource_id}/tags                                            | er:tags:get                         | -            |
| POST /v3/{project_id}/{resource_type}/{resource_id}/tags                                           | er:tags:singleCreate                | -            |
| POST /v3/{project_id}/{resource_type}/{resource_id}/tags/action                                    | er:tags:batchOperation              | -            |
| DELETE /v3/{project_id}/{resource_type}/{resource_id}/tags/{key}                                   | er:tags:delete                      | -            |
| GET /v3/{project_id}/enterprise-router/quotas                                                      | er:quotas:list                      | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs                                          | er:flowLogs:create                  | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/flow-logs                                           | er:flowLogs:list                    | -            |
| GET /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}                             | er:flowLogs:get                     | -            |

| API                                                                             | Action              | Dependencies |
|---------------------------------------------------------------------------------|---------------------|--------------|
| PUT /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}          | er:flowLogs:update  | -            |
| DELETE /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}       | er:flowLogs:delete  | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}/enable  | er:flowLogs:enable  | -            |
| POST /v3/{project_id}/enterprise-router/{er_id}/flow-logs/{flow_log_id}/disable | er:flowLogs:disable | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-42](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for er.

**Table 3-42** Resource types supported by er

| Resource Type | URN                                                   |
|---------------|-------------------------------------------------------|
| instances     | er:<region>:<account-id>:instances:<instance-id>      |
| routeTables   | er:<region>:<account-id>:routeTables:<route-table-id> |
| flowLogs      | er:<region>:<account-id>:flowLogs:<flow-log-id>       |
| attachments   | er:<region>:<account-id>:attachments:<attachment-id>  |

## Conditions

er does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.3.2 Virtual Private Cloud

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by vpc, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by vpc, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for vpc.

**Table 3-43** Actions supported by vpc

| Action          | Description                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                       | Alias |
|-----------------|----------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:vpcs:create | Grants permission to create vpc. | Write        | vpc *                       | -                                                                                                                                                                                                                                                   | -     |
|                 |                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">vpc:VpcBlockServiceEndpointStates</a></li> </ul> |       |
| vpc:vpcs:get    | Grants permission to get vpc.    | Read         | vpc *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                             | -     |
| vpc:vpcs:list   | Grants permission to list vpc.   | List         | vpc *                       | -                                                                                                                                                                                                                                                   | -     |
|                 |                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                               |       |
| vpc:vpcs:update | Grants permission to update vpc. | Write        | vpc *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                             | -     |
|                 |                                  |              | -                           | <a href="#">vpc:VpcBlockServiceEndpointStates</a>                                                                                                                                                                                                   |       |

| Action             | Description                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                   | Alias |
|--------------------|-------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:vpcs:delete    | Grants permission to delete vpc.    | Write        | vpc *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                                                         | -     |
| vpc:subnets:create | Grants permission to create subnet. | Write        | subnet *                    | -                                                                                                                                                                                                                                                                               | -     |
|                    |                                     |              | vpc *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                                                         |       |
|                    |                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">vpc:AvailabilityZone</a></li> <li>• <a href="#">vpc:SubnetIpv6Enable</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                           |       |
| vpc:subnets:get    | Grants permission to get subnet.    | Read         | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">vpc:AvailabilityZone</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |



| Action                        | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                         | Alias           |
|-------------------------------|--------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| vpc:subnets:list              | Grants permission to list subnets.                     | List         | subnet *                    | -                                                                                                                                                                                                                                                                     | vpc:subnets:get |
|                               |                                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                 |                 |
| vpc:subnets:update            | Grants permission to update subnet.                    | Write        | subnet *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">vpc:SubnetId</a></li> <li><a href="#">vpc:VpcId</a></li> <li><a href="#">vpc:AvailabilityZone</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -               |
|                               |                                                        |              | -                           | <a href="#">vpc:SubnetIpv6Enable</a>                                                                                                                                                                                                                                  |                 |
| vpc:subnets:delete            | Grants permission to delete subnet.                    | Write        | subnet *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">vpc:SubnetId</a></li> <li><a href="#">vpc:VpcId</a></li> <li><a href="#">vpc:AvailabilityZone</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -               |
| vpc:subnets:createReservation | Grants permission to create a subnet cidr reservation. | Write        | subnet *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                        | -               |

| Action                        | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                 | Alias          |
|-------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| vpc:subnets:getReservation    | Grants permission to get a subnet cidr reservation.    | Read         | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VirusubnetCidrReservationId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -              |
| vpc:subnets:listReservations  | Grants permission to list subnet cidr reservation.     | List         | subnet *                    | -                                                                                                                                                                                                             | -              |
|                               |                                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                         |                |
| vpc:subnets:updateReservation | Grants permission to update a subnet cidr reservation. | Write        | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VirusubnetCidrReservationId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -              |
| vpc:subnets:deleteReservation | Grants permission to delete a subnet cidr reservation. | Write        | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VirusubnetCidrReservationId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -              |
| vpc:quotas:list               | Grants permission to list quotas.                      | List         | -                           | -                                                                                                                                                                                                             | vpc:quotas:get |

| Action                    | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                  | Alias |
|---------------------------|--------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:privatelps:create     | Grants permission to create private.       | Write        | privatelp *                 | -                                                                                                                                                                                                                              | -     |
|                           |                                            |              | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">vpc:AvailabilityZone</a></li> </ul> |       |
| vpc:privatelps:get        | Grants permission to get privateip.        | Read         | privatelp *                 | <ul style="list-style-type: none"> <li>• <a href="#">vpc:PrivateIpId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                               | -     |
| vpc:privatelps:list       | Grants permission to list privateip.       | List         | privatelp *                 | -                                                                                                                                                                                                                              | -     |
| vpc:privatelps:delete     | Grants permission to delete privateip.     | Write        | privatelp *                 | <ul style="list-style-type: none"> <li>• <a href="#">vpc:PrivateIpId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                               | -     |
| vpc:securityGroups:create | Grants permission to create securityGroup. | Write        | securityGroup *             | -                                                                                                                                                                                                                              | -     |

| Action | Description | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                           | Alias |
|--------|-------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|        |             |              | securityGroupRule           | <ul style="list-style-type: none"><li>vpc:SecurityGroupRuleDirection</li><li>vpc:SecurityGroupRuleProtocol</li><li>vpc:SecurityGroupRuleAction</li><li>vpc:SecurityGroupRulePort</li><li>vpc:SecurityGroupRuleRemoteIpAddressGroup</li><li>vpc:SecurityGroupRuleRemoteSecurityGroup</li><li>vpc:SecurityGroupRuleRemotePrefix</li></ul> |       |
|        |             |              | -                           | <ul style="list-style-type: none"><li>g:EnterpriseProjectId</li><li>g:RequestTag/&lt;tag-key&gt;</li><li>g:TagKeys</li></ul>                                                                                                                                                                                                            |       |

| Action                    | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                     | Alias                  |
|---------------------------|--------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| vpc:securityGroups:get    | Grants permission to get securityGroup.    | Read         | securityGroup *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">vpc:SecurityGroupId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                      |
| vpc:securityGroups:list   | Grants permission to list securityGroups.  | List         | securityGroup *             | -                                                                                                                                                                                                 | vpc:securityGroups:get |
|                           |                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                             |                        |
| vpc:securityGroups:update | Grants permission to update securityGroup. | Write        | securityGroup *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">vpc:SecurityGroupId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                      |
| vpc:securityGroups:delete | Grants permission to delete securityGroup. | Write        | securityGroup *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">vpc:SecurityGroupId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                      |

| Action                        | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Alias |
|-------------------------------|-------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:securityGroupRules:create | Grants permission to create securityGroup Rule. | Write        | securityGroupRule *         | <ul style="list-style-type: none"> <li>• <a href="#">vpc:SecurityGroupRuleDirection</a></li> <li>• <a href="#">vpc:SecurityGroupRuleProtocol</a></li> <li>• <a href="#">vpc:SecurityGroupRuleAction</a></li> <li>• <a href="#">vpc:SecurityGroupRulePort</a></li> <li>• <a href="#">vpc:SecurityGroupRuleRemoteIpAddressGroup</a></li> <li>• <a href="#">vpc:SecurityGroupRuleRemoteSecurityGroup</a></li> <li>• <a href="#">vpc:SecurityGroupRuleRemotePrefix</a></li> </ul> | -     |
|                               |                                                 |              | securityGroup *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">vpc:SecurityGroupId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                                                                                             |       |
| vpc:securityGroupRules:get    | Grants permission to get securityGroup Rule.    | Read         | securityGroupRule *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">vpc:SecurityGroupId</a></li> </ul>                                                                                                                                                                                                                                                                                                                                      | -     |

| Action                        | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Alias                      |
|-------------------------------|-------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| vpc:securityGroupRules:list   | Grants permission to list securityGroup Rules.  | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                           | vpc:securityGroupRules:get |
| vpc:securityGroupRules:update | Grants permission to update securityGroup Rule. | Write        | securityGroupRule *         | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">vpc:SecurityGroupId</a></li> </ul>                                                                                                                                                                                                                                                                                                                            | -                          |
|                               |                                                 |              | -                           | <ul style="list-style-type: none"> <li><a href="#">vpc:SecurityGroupRuleDirection</a></li> <li><a href="#">vpc:SecurityGroupRuleProtocol</a></li> <li><a href="#">vpc:SecurityGroupRuleAction</a></li> <li><a href="#">vpc:SecurityGroupRulePort</a></li> <li><a href="#">vpc:SecurityGroupRuleRemoteIpAddressGroup</a></li> <li><a href="#">vpc:SecurityGroupRuleRemoteSecurityGroup</a></li> <li><a href="#">vpc:SecurityGroupRuleRemotePrefix</a></li> </ul> |                            |

| Action                        | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                         | Alias         |
|-------------------------------|-------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| vpc:securityGroupRules:delete | Grants permission to delete securityGroup Rule. | Write        | securityGroupRule *         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>vpc:SecurityGroupId</li> </ul>                                                                                  | -             |
| vpc:ports:create              | Grants permission to create port.               | Write        | port *                      | -                                                                                                                                                                                     | -             |
|                               |                                                 |              | subnet *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>vpc:SubnetId</li> <li>vpc:VpcId</li> <li>vpc:AvailabilityZone</li> <li>g:EnterpriseProjectId</li> </ul> |               |
|                               |                                                 |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                                                                                     |               |
| vpc:ports:get                 | Grants permission to get port.                  | Read         | port *                      | <ul style="list-style-type: none"> <li>vpc:SubnetId</li> <li>vpc:PortId</li> <li>vpc:VpcId</li> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>           | -             |
| vpc:ports:list                | Grants permission to list ports.                | List         | port *                      | -                                                                                                                                                                                     | vpc:ports:get |
|                               |                                                 |              | -                           | g:EnterpriseProjectId                                                                                                                                                                 |               |



| Action              | Description                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                         | Alias           |
|---------------------|--------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| vpc:ports:update    | Grants permission to update port.    | Write        | port *                      | <ul style="list-style-type: none"> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:PortId</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:vips:update |
| vpc:ports:delete    | Grants permission to delete port.    | Write        | port *                      | <ul style="list-style-type: none"> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:PortId</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -               |
| vpc:peerings:create | Grants permission to create peering. | Write        | peerings *                  | <ul style="list-style-type: none"> <li>• <a href="#">vpc:AccepterVpcId</a></li> <li>• <a href="#">vpc:RequesterVpcId</a></li> <li>• <a href="#">vpc:AccepterVpcOrgPath</a></li> <li>• <a href="#">vpc:AccepterVpcOwner</a></li> </ul>                                 | -               |
|                     |                                      |              | vpc *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                                                                                                |                 |

| Action                  | Description                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                   | Alias                |
|-------------------------|--------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| vpc:peerings:get        | Grants permission to get peering.    | Read         | peeri<br>ng *               | <ul style="list-style-type: none"> <li>• <a href="#">vpc:AccepterVpcId</a></li> <li>• <a href="#">vpc:RequesterVpcId</a></li> <li>• <a href="#">vpc:Peerin<br/>gId</a></li> </ul>                                                                                                               | -                    |
| vpc:peerings:li<br>st   | Grants permission to list peerings.  | List         | peeri<br>ng *               | -                                                                                                                                                                                                                                                                                               | vpc:peerings:g<br>et |
| vpc:peerings:a<br>ccept | Grants permission to accept peering. | Write        | peeri<br>ng *               | <ul style="list-style-type: none"> <li>• <a href="#">vpc:AccepterVpcId</a></li> <li>• <a href="#">vpc:RequesterVpcId</a></li> <li>• <a href="#">vpc:Peerin<br/>gId</a></li> <li>• <a href="#">vpc:RequesterVpcOr<br/>gPath</a></li> <li>• <a href="#">vpc:RequesterVpcO<br/>wner</a></li> </ul> | -                    |
| vpc:peerings:r<br>eject | Grants permission to reject peering. | Write        | peeri<br>ng *               | <ul style="list-style-type: none"> <li>• <a href="#">vpc:AccepterVpcId</a></li> <li>• <a href="#">vpc:RequesterVpcId</a></li> <li>• <a href="#">vpc:Peerin<br/>gId</a></li> </ul>                                                                                                               | -                    |
| vpc:peerings:u<br>pdate | Grants permission to update peering. | Write        | peeri<br>ng *               | <ul style="list-style-type: none"> <li>• <a href="#">vpc:AccepterVpcId</a></li> <li>• <a href="#">vpc:RequesterVpcId</a></li> <li>• <a href="#">vpc:Peerin<br/>gId</a></li> </ul>                                                                                                               | -                    |

| Action                    | Description                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|---------------------------|----------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:peerings:delete       | Grants permission to delete peering.         | Write        | peering *                   | <ul style="list-style-type: none"> <li>vpc:AccepterVpcId</li> <li>vpc:RequesterVpcId</li> <li>vpc:PeerIngId</li> </ul>            | -     |
| vpc:routeTables:create    | Grants permission to create routeTable.      | Write        | routeTable *                | -                                                                                                                                 | -     |
|                           |                                              |              | vpc *                       | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>vpc:VpcId</li> </ul> |       |
| vpc:routeTables:get       | Grants permission to get routeTable.         | Read         | routeTable *                | <ul style="list-style-type: none"> <li>vpc:RouteTableId</li> <li>vpc:VpcId</li> <li>g:EnterpriseProjectId</li> </ul>              | -     |
| vpc:routeTables:list      | Grants permission to list routeTables.       | List         | routeTable *                | -                                                                                                                                 | -     |
|                           |                                              |              | -                           | g:EnterpriseProjectId                                                                                                             |       |
| vpc:routeTables:update    | Grants permission to update routeTable.      | Write        | routeTable *                | <ul style="list-style-type: none"> <li>vpc:RouteTableId</li> <li>vpc:VpcId</li> <li>g:EnterpriseProjectId</li> </ul>              | -     |
| vpc:routeTables:associate | Grants permission to associate a routeTable. | Write        | routeTable *                | <ul style="list-style-type: none"> <li>vpc:RouteTableId</li> <li>vpc:VpcId</li> </ul>                                             | -     |

| Action                 | Description                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                         | Alias |
|------------------------|-----------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                        |                                         |              | subnet *                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>vpc:SubnetId</li> <li>vpc:VpcId</li> <li>vpc:AvailabilityZone</li> <li>g:EnterpriseProjectId</li> </ul> |       |
| vpc:routeTables:delete | Grants permission to delete routeTable. | Write        | routeTable *                | <ul style="list-style-type: none"> <li>vpc:RouteTableId</li> <li>vpc:VpcId</li> <li>g:EnterpriseProjectId</li> </ul>                                                                  | -     |
| vpc:flowLogs:create    | Grants permission to create flowLog.    | Write        | flowLog *                   | -                                                                                                                                                                                     | -     |
|                        |                                         |              | port                        | <ul style="list-style-type: none"> <li>vpc:PortId</li> <li>vpc:SubnetId</li> <li>vpc:VpcId</li> </ul>                                                                                 |       |
|                        |                                         |              | subnet                      | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>vpc:SubnetId</li> <li>vpc:VpcId</li> <li>vpc:AvailabilityZone</li> </ul>                                |       |
|                        |                                         |              | vpc                         | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>vpc:VpcId</li> </ul>                                                                                    |       |
|                        |                                         |              | -                           | vpc:FlogLogResourceType                                                                                                                                                               |       |

| Action                   | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                              | Alias            |
|--------------------------|-------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| vpc:flowLogs:get         | Grants permission to get flowLog.         | Read         | flowLog *                   | <ul style="list-style-type: none"> <li>vpc:FlowLogId</li> <li>vpc:FlowLogResourceType</li> </ul>                                           | -                |
| vpc:flowLogs:list        | Grants permission to list flowLog.        | List         | flowLog *                   | -                                                                                                                                          | vpc:flowLogs:get |
| vpc:flowLogs:update      | Grants permission to update flowLog.      | Write        | flowLog *                   | <ul style="list-style-type: none"> <li>vpc:FlowLogId</li> <li>vpc:FlowLogResourceType</li> </ul>                                           | -                |
| vpc:flowLogs:delete      | Grants permission to delete flowLog.      | Write        | flowLog *                   | <ul style="list-style-type: none"> <li>vpc:FlowLogId</li> <li>vpc:FlowLogResourceType</li> </ul>                                           | -                |
| vpc:addressGroups:create | Grants permission to create addressGroup. | Write        | addressGroup *              | -                                                                                                                                          | -                |
|                          |                                           |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>           |                  |
| vpc:addressGroups:get    | Grants permission to get addressGroup.    | Read         | addressGroup *              | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>vpc:AddressGroupId</li> </ul> | -                |

| Action                   | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                              | Alias |
|--------------------------|-------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:addressGroups:list   | Grants permission to list addressGroup.   | List         | addressGroup *              | -                                                                                                                                                                                          | -     |
|                          |                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                      |       |
| vpc:addressGroups:update | Grants permission to update addressGroup. | Write        | addressGroup *              | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">vpc:AddressGroupId</a></li> </ul> | -     |
| vpc:addressGroups:delete | Grants permission to delete addressGroup. | Write        | addressGroup *              | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">vpc:AddressGroupId</a></li> </ul> | -     |
| vpc:firewalls:create     | Grants permission to create firewall.     | Write        | firewall *                  | -                                                                                                                                                                                          | -     |
|                          |                                           |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>           |       |
| vpc:firewalls:get        | Grants permission to get firewall.        | Read         | firewall *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">vpc:FirewallId</a></li> </ul>     | -     |

| Action             | Description                         | Access Level | Resource Type (*: required) | Condition Key                | Alias |
|--------------------|-------------------------------------|--------------|-----------------------------|------------------------------|-------|
| vpc:firewalls:list | Grants permission to list firewall. | List         | firewall *                  | -                            | -     |
|                    |                                     |              | -                           | <b>g:EnterpriseProjectId</b> |       |

| Action               | Description                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Alias |
|----------------------|---------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:firewalls:update | Grants permission to update firewall. | Write        | firewall *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:FirewallId</a></li> <li>• <a href="#">vpc:FirewallRuleDirection</a></li> <li>• <a href="#">vpc:FirewallRuleProtocol</a></li> <li>• <a href="#">vpc:FirewallRuleAction</a></li> <li>• <a href="#">vpc:FirewallRuleSourcePort</a></li> <li>• <a href="#">vpc:FirewallRuleDestinationPort</a></li> <li>• <a href="#">vpc:FirewallOperationType</a></li> <li>• <a href="#">vpc:FirewallRuleSourceIp</a></li> <li>• <a href="#">vpc:FirewallRuleSourceIpAddressGroup</a></li> <li>• <a href="#">vpc:FirewallRuleDestinationIp</a></li> <li>• <a href="#">vpc:FirewallRuleDestinationIpAddressGroup</a></li> </ul> | -     |



| Action               | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                   | Alias              |
|----------------------|-----------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
|                      |                                                     |              | subnet                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">vpc:AvailabilityZone</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                    |
| vpc:firewalls:delete | Grants permission to delete firewall.               | Write        | firewall *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:FirewallId</a></li> </ul>                                                                                    | -                  |
| vpc:vpcs:createTags  | Grants permission to create a tag for an vpc.       | Tagging      | vpc *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                                                         | vpc:vpcTags:create |
|                      |                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                           |                    |
| vpc:vpcs:listTags    | Grants permission to query tags of a specified vpc. | List         | vpc *                       | -                                                                                                                                                                                                                                                                               | vpc:vpcTags:get    |

| Action                 | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                   | Alias                 |
|------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| vpc:vpcs:deleteTags    | Grants permission to delete an vpc tag.                | Tagging      | vpc *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                                                                                         | vpc:vpcTags:delete    |
|                        |                                                        |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                                       |                       |
| vpc:subnets:createTags | Grants permission to create a tag for an subnet.       | Tagging      | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:AvailabilityZone</a></li> </ul> | vpc:subnetTags:create |
|                        |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                           |                       |
| vpc:subnets:listTags   | Grants permission to query tags of a specified subnet. | List         | subnet *                    | -                                                                                                                                                                                                                                                                               | vpc:subnetTags:get    |

| Action                       | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                   | Alias                       |
|------------------------------|--------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| vpc:subnets:deleteTags       | Grants permission to delete an subnet tag.                   | Tagging      | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:AvailabilityZone</a></li> </ul> | vpc:subnetTags:delete       |
|                              |                                                              |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                                       |                             |
| vpc:addressGroups:createTags | Grants permission to create a tag for an addressGroup.       | Tagging      | addressGroup *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:AddressGroupId</a></li> </ul>                                                                                | vpc:addressGroupTags:create |
|                              |                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                           |                             |
| vpc:addressGroups:listTags   | Grants permission to query tags of a specified addressGroup. | List         | addressGroup *              | -                                                                                                                                                                                                                                                                               | vpc:addressGroupTags:get    |
| vpc:addressGroups:deleteTags | Grants permission to delete an addressGroup tag.             | Tagging      | addressGroup *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:AddressGroupId</a></li> </ul>                                                                                | vpc:addressGroupTags:delete |
|                              |                                                              |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                                       |                             |

| Action                        | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                     | Alias                        |
|-------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| vpc:securityGroups:createTags | Grants permission to create a tag for a securityGroup.        | Tagging      | securityGroup *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SecurityGroupId</a></li> </ul> | vpc:securityGroupTags:create |
|                               |                                                               |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                             |                              |
| vpc:securityGroups:listTags   | Grants permission to query tags of a specified securityGroup. | List         | securityGroup *             | -                                                                                                                                                                                                 | vpc:securityGroupTags:get    |
| vpc:securityGroups:deleteTags | Grants permission to delete a securityGroup tag.              | Tagging      | securityGroup *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SecurityGroupId</a></li> </ul> | vpc:securityGroupTags:delete |
|                               |                                                               |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                         |                              |
| vpc:firewalls:createTags      | Grants permission to create a tag for a firewall.             | Tagging      | firewall *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:FirewallId</a></li> </ul>      | vpc:firewallTags:create      |
|                               |                                                               |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                             |                              |

| Action                              | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                        | Alias                              |
|-------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| vpc:firewalls:listTags              | Grants permission to query tags of a specified firewall.            | List         | firewall *                  | -                                                                                                                                                                                                                                                                                    | vpc:firewallTags:get               |
| vpc:firewalls:deleteTags            | Grants permission to delete an firewall tag.                        | Tagging      | firewall *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:FirewallId</a></li> </ul>                                                                                         | vpc:firewallTags:delete            |
|                                     |                                                                     |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                                            |                                    |
| vpc:subNetworkInterfaces:createTags | Grants permission to create a tag for a subNetworkInterface.        | Tagging      | subNetworkInterface *       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubNetworkInterfaceId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul> | vpc:subNetworkInterfaceTags:create |
|                                     |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                                |                                    |
| vpc:subNetworkInterfaces:listTags   | Grants permission to query tags of a specified subNetworkInterface. | List         | subNetworkInterface *       | -                                                                                                                                                                                                                                                                                    | vpc:subNetworkInterfaceTags:get    |

| Action                              | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                        | Alias                              |
|-------------------------------------|--------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| vpc:subNetworkInterfaces:deleteTags | Grants permission to delete a subNetworkInterface tag. | Tagging      | subNetworkInterface *       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubNetworkInterfaceId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul> | vpc:subNetworkInterfaceTags:delete |
|                                     |                                                        |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                                            |                                    |
| vpc:ports:createTags                | Grants permission to create a tag for a port.          | Tagging      | port *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:PortId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul>                | vpc:portTags:create                |
|                                     |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                                |                                    |
| vpc:ports:listTags                  | Grants permission to query tags of a specified port.   | List         | port *                      | -                                                                                                                                                                                                                                                                                    | vpc:portTags:get                   |

| Action                          | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                         | Alias               |
|---------------------------------|--------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| vpc:ports:deleteTags            | Grants permission to delete a port tag.          | Tagging      | port *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:PortId</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul> | vpc:portTags:delete |
|                                 |                                                  |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                             |                     |
| vpc:subNetworkInterfaces:create | Grants permission to create subNetworkInterface. | Write        | subNetworkInterface *       | -                                                                                                                                                                                                                                                                     | -                   |
|                                 |                                                  |              | subnet *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:VpcId</a></li> <li>• <a href="#">vpc:AvailabilityZone</a></li> </ul>                                        |                     |
|                                 |                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                |                     |

| Action                          | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                        | Alias |
|---------------------------------|--------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:subNetworkInterfaces:get    | Grants permission to get subNetworkInterface.    | Read         | subNetworkInterface *       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:SubNetworkInterfaceId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul> | -     |
| vpc:subNetworkInterfaces:list   | Grants permission to list subNetworkInterface.   | List         | subNetworkInterface *       | -                                                                                                                                                                                                                                                                                    | -     |
|                                 |                                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                |       |
| vpc:subNetworkInterfaces:update | Grants permission to update subNetworkInterface. | Write        | subNetworkInterface *       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:SubNetworkInterfaceId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul> | -     |



| Action                          | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                        | Alias            |
|---------------------------------|--------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| vpc:subNetworkInterfaces:delete | Grants permission to delete subNetworkInterface. | Write        | subNetworkInterface *       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">vpc:SubnetId</a></li> <li>• <a href="#">vpc:SubNetworkInterfaceId</a></li> <li>• <a href="#">vpc:VpcId</a></li> </ul> | -                |
| vpc:networks:create             | Grants permission to create network.             | Write        | network *                   | -                                                                                                                                                                                                                                                                                    | -                |
| vpc:networks:get                | Grants permission to get network.                | Read         | network *                   | -                                                                                                                                                                                                                                                                                    | -                |
| vpc:networks:list               | Grants permission to list network.               | List         | network *                   | -                                                                                                                                                                                                                                                                                    | vpc:networks:get |
| vpc:networks:update             | Grants permission to update network.             | Write        | network *                   | -                                                                                                                                                                                                                                                                                    | -                |
| vpc:networks:delete             | Grants permission to delete network.             | Write        | addressGroup *              | -                                                                                                                                                                                                                                                                                    | -                |
| vpc:trafficMirrorFilters:create | Grants permission to create trafficMirrorFilter. | Write        | trafficMirrorFilter *       | -                                                                                                                                                                                                                                                                                    | -                |

| Action                              | Description                                          | Access Level | Resource Type (*: required) | Condition Key                    | Alias |
|-------------------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------|-------|
| vpc:trafficMirrorFilters:get        | Grants permission to get trafficMirrorFilter.        | Read         | trafficMirrorFilter *       | -                                | -     |
| vpc:trafficMirrorFilters:list       | Grants permission to list trafficMirrorFilter.       | List         | trafficMirrorFilter *       | -                                | -     |
| vpc:trafficMirrorFilters:update     | Grants permission to update trafficMirrorFilter.     | Write        | trafficMirrorFilter *       | -                                | -     |
| vpc:trafficMirrorFilters:delete     | Grants permission to delete trafficMirrorFilter.     | Write        | trafficMirrorFilter *       | -                                | -     |
| vpc:trafficMirrorFilterRules:create | Grants permission to create trafficMirrorFilterRule. | Write        | trafficMirrorFilter *       | -                                | -     |
|                                     |                                                      |              | trafficMirrorFilterRule *   | -                                |       |
| vpc:trafficMirrorFilterRules:get    | Grants permission to get trafficMirrorFilterRule.    | Read         | trafficMirrorFilterRule *   | <b>vpc:TrafficMirrorFilterId</b> | -     |
| vpc:trafficMirrorFilterRules:list   | Grants permission to list trafficMirrorFilterRule.   | List         | trafficMirrorFilterRule *   | -                                | -     |

| Action                              | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                  | Alias |
|-------------------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:trafficMirrorFilterRules:update | Grants permission to update trafficMirrorFilterRule. | Write        | trafficMirrorFilterRule *   | <b>vpc:TrafficMirrorFilterId</b>                                                                                                                                                                                                                               | -     |
| vpc:trafficMirrorFilterRules:delete | Grants permission to delete trafficMirrorFilterRule. | Write        | trafficMirrorFilterRule *   | <b>vpc:TrafficMirrorFilterId</b>                                                                                                                                                                                                                               | -     |
| vpc:trafficMirrorSessions:create    | Grants permission to create trafficMirrorSession.    | Write        | trafficMirrorSession *      | <ul style="list-style-type: none"> <li><b>vpc:TrafficMirrorTargetType</b></li> <li><b>vpc:TrafficMirrorTargetId</b></li> <li><b>vpc:TrafficMirrorSourceType</b></li> <li><b>vpc:TrafficMirrorSourceId</b></li> <li><b>vpc:TrafficMirrorFilterId</b></li> </ul> | -     |
|                                     |                                                      |              | trafficMirrorFilter *       | -                                                                                                                                                                                                                                                              |       |

| Action                           | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                         | Alias |
|----------------------------------|---------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:trafficMirrorSessions:get    | Grants permission to get trafficMirrorSession.    | Read         | trafficMirrorSession *      | <ul style="list-style-type: none"> <li>• <a href="#">vpc:TrafficMirrorTargetType</a></li> <li>• <a href="#">vpc:TrafficMirrorTargetId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceType</a></li> <li>• <a href="#">vpc:TrafficMirrorFilterId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceId</a></li> </ul> | -     |
| vpc:trafficMirrorSessions:list   | Grants permission to list trafficMirrorSession.   | List         | trafficMirrorSession *      | -                                                                                                                                                                                                                                                                                                                     | -     |
| vpc:trafficMirrorSessions:update | Grants permission to update trafficMirrorSession. | Write        | trafficMirrorSession *      | <ul style="list-style-type: none"> <li>• <a href="#">vpc:TrafficMirrorTargetType</a></li> <li>• <a href="#">vpc:TrafficMirrorTargetId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceType</a></li> <li>• <a href="#">vpc:TrafficMirrorFilterId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceId</a></li> </ul> | -     |
|                                  |                                                   |              | trafficMirrorFilter         | -                                                                                                                                                                                                                                                                                                                     |       |

| Action                                 | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                         | Alias |
|----------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:trafficMirrorSessions:addSource    | Grants permission to add trafficMirrorSession source resource.    | Write        | trafficMirrorSession *      | <ul style="list-style-type: none"> <li>• <a href="#">vpc:TrafficMirrorTargetType</a></li> <li>• <a href="#">vpc:TrafficMirrorTargetId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceType</a></li> <li>• <a href="#">vpc:TrafficMirrorFilterId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceId</a></li> </ul> | -     |
| vpc:trafficMirrorSessions:removeSource | Grants permission to remove trafficMirrorSession source resource. | Write        | trafficMirrorSession *      | <ul style="list-style-type: none"> <li>• <a href="#">vpc:TrafficMirrorTargetType</a></li> <li>• <a href="#">vpc:TrafficMirrorTargetId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceType</a></li> <li>• <a href="#">vpc:TrafficMirrorFilterId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceId</a></li> </ul> | -     |

| Action                           | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                         | Alias |
|----------------------------------|---------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpc:trafficMirrorSessions:delete | Grants permission to delete trafficMirrorSession. | Write        | trafficMirrorSession *      | <ul style="list-style-type: none"> <li>• <a href="#">vpc:TrafficMirrorTargetType</a></li> <li>• <a href="#">vpc:TrafficMirrorTargetId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceType</a></li> <li>• <a href="#">vpc:TrafficMirrorFilterId</a></li> <li>• <a href="#">vpc:TrafficMirrorSourceId</a></li> </ul> | -     |

Each API of vpc usually supports one or more actions. [Table 3-44](#) lists the supported actions and dependencies.

**Table 3-44** Actions and dependencies supported by vpc APIs

| API                                   | Action             | Dependencies |
|---------------------------------------|--------------------|--------------|
| POST /v1/{project_id}/vpcs            | vpc:vpcs:create    | -            |
| GET /v1/{project_id}/vpcs/{vpc_id}    | vpc:vpcs:get       | -            |
| GET /v1/{project_id}/vpcs             | vpc:vpcs:list      | -            |
| PUT /v1/{project_id}/vpcs/{vpc_id}    | vpc:vpcs:update    | -            |
| DELETE /v1/{project_id}/vpcs/{vpc_id} | vpc:vpcs:delete    | -            |
| POST /v1/{project_id}/subnets         | vpc:subnets:create | -            |

| API                                                       | Action                    | Dependencies |
|-----------------------------------------------------------|---------------------------|--------------|
| GET /v1/{project_id}/subnets/{subnet_id}                  | vpc:subnets:get           | -            |
| GET /v1/{project_id}/subnets                              | vpc:subnets:list          | -            |
| PUT /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id}    | vpc:subnets:update        | -            |
| DELETE /v1/{project_id}/vpcs/{vpc_id}/subnets/{subnet_id} | vpc:subnets:delete        | -            |
| GET /v1/{project_id}/quotas                               | vpc:quotas:list           | -            |
| POST /v1/{project_id}/privateips                          | vpc:privateips:create     | -            |
| GET /v1/{project_id}/privateips/{privateip_id}            | vpc:privateips:get        | -            |
| GET /v1/{project_id}/subnets/{subnet_id}/privateips       | vpc:privateips:list       | -            |
| DELETE /v1/{project_id}/privateips/{privateip_id}         | vpc:privateips:delete     | -            |
| POST /v1/{project_id}/security-groups                     | vpc:securityGroups:create | -            |
| GET /v1/{project_id}/security-groups/{security_group_id}  | vpc:securityGroups:get    | -            |
| GET /v1/{project_id}/security-groups                      | vpc:securityGroups:list   | -            |

| API                                                                                             | Action                        | Dependencies |
|-------------------------------------------------------------------------------------------------|-------------------------------|--------------|
| DELETE /v1/{project_id}/security-groups/{security_group_id}                                     | vpc:securityGroups:delete     | -            |
| POST /v1/{project_id}/security-group-rules                                                      | vpc:securityGroupRules:create | -            |
| POST /v3/{project_id}/vpc/security-groups/{security_group_id}/security-group-rules/batch-create | vpc:securityGroupRules:create | -            |
| GET /v1/{project_id}/security-group-rules/{security_group_rule_id}                              | vpc:securityGroupRules:get    | -            |
| GET /v1/{project_id}/security-group-rules                                                       | vpc:securityGroupRules:list   | -            |
| DELETE /v1/{project_id}/security-group-rules/{security_group_rule_id}                           | vpc:securityGroupRules:delete | -            |
| POST /v1/{project_id}/ports                                                                     | vpc:ports:create              | -            |
| GET /v1/{project_id}/ports/{port_id}                                                            | vpc:ports:get                 | -            |
| GET /v1/{project_id}/ports                                                                      | vpc:ports:list                | -            |
| PUT /v1/{project_id}/ports/{port_id}                                                            | vpc:ports:update              | -            |
| DELETE /v1/{project_id}/ports/{port_id}                                                         | vpc:ports:delete              | -            |
| POST /v2.0/vpc/peerings                                                                         | vpc:peerings:create           | -            |



| API                                                         | Action                    | Dependencies |
|-------------------------------------------------------------|---------------------------|--------------|
| PUT /v2.0/vpc/peerings/{peering_id}/accept                  | vpc:peerings:accept       | -            |
| PUT /v2.0/vpc/peerings/{peering_id}/reject                  | vpc:peerings:reject       | -            |
| GET /v2.0/vpc/peerings/{peering_id}                         | vpc:peerings:get          | -            |
| GET /v2.0/vpc/peerings                                      | vpc:peerings:list         | -            |
| PUT /v2.0/vpc/peerings/{peering_id}                         | vpc:peerings:update       | -            |
| DELETE /v2.0/vpc/peerings/{peering_id}                      | vpc:peerings:delete       | -            |
| POST /v1/{project_id}/routetables                           | vpc:routetables:create    | -            |
| GET /v1/{project_id}/routetables/{routetable_id}            | vpc:routetables:get       | -            |
| GET /v1/{project_id}/routetables                            | vpc:routetables:list      | -            |
| PUT /v1/{project_id}/routetables/{routetable_id}            | vpc:routetables:update    | -            |
| POST /v1/{project_id}/routetables/{routetable_id}/action    | vpc:routetables:associate | -            |
| POST 01 /v1/{project_id}/routetables/{routetable_id}/action | vpc:routetables:associate | -            |

| API                                                                      | Action                    | Dependencies |
|--------------------------------------------------------------------------|---------------------------|--------------|
| DELETE /v1/<br>{project_id}/<br>routetables/<br>{routetable_id}          | vpc:routetables:delete    | -            |
| POST /v1/<br>{project_id}/fl/<br>flow_logs                               | vpc:flowLogs:create       | -            |
| GET /v1/<br>{project_id}/fl/<br>flow_logs/<br>{flowlog_id}               | vpc:flowLogs:get          | -            |
| GET /v1/<br>{project_id}/fl/<br>flow_logs                                | vpc:flowLogs:list         | -            |
| PUT /v1/<br>{project_id}/fl/<br>flow_logs/<br>{flowlog_id}               | vpc:flowLogs:update       | -            |
| DELETE /v1/<br>{project_id}/fl/<br>flow_logs/<br>{flowlog_id}            | vpc:flowLogs:delete       | -            |
| PUT /v3/<br>{project_id}/vpc/<br>vpcs/{vpc_id}/add-<br>extend-cidr       | vpc:vpcs:update           | -            |
| PUT /v3/<br>{project_id}/vpc/<br>vpcs/{vpc_id}/<br>remove-extend-cidr    | vpc:vpcs:update           | -            |
| PUT /v3/<br>{project_id}/vpc/<br>security-groups/<br>{security_group_id} | vpc:securityGroups:update | -            |
| POST /v3/<br>{project_id}/vpc/<br>address-groups                         | vpc:addressGroups:create  | -            |
| GET /v3/<br>{project_id}/vpc/<br>address-groups/<br>{address_group_id}   | vpc:addressGroups:get     | -            |

| API                                                                                   | Action                   | Dependencies |
|---------------------------------------------------------------------------------------|--------------------------|--------------|
| GET /v3/<br>{project_id}/vpc/<br>address-groups                                       | vpc:addressGroups:list   | -            |
| PUT /v3/<br>{project_id}/vpc/<br>address-groups/<br>{address_group_id}                | vpc:addressGroups:update | -            |
| DELETE /v3/<br>{project_id}/vpc/<br>address-groups/<br>{address_group_id}             | vpc:addressGroups:delete | -            |
| DELETE /v3/<br>{project_id}/vpc/<br>address-groups/<br>{address_group_id}/<br>force   | vpc:addressGroups:delete | -            |
| POST /v3/<br>{project_id}/vpc/<br>firewalls                                           | vpc:firewalls:create     | -            |
| PUT /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}                          | vpc:firewalls:update     | -            |
| PUT /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}/<br>associate-subnets    | vpc:firewalls:update     | -            |
| PUT /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}/<br>disassociate-subnets | vpc:firewalls:update     | -            |
| PUT /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}/insert-<br>rules         | vpc:firewalls:update     | -            |
| PUT /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}/<br>remove-rules         | vpc:firewalls:update     | -            |

| API                                                                           | Action                 | Dependencies |
|-------------------------------------------------------------------------------|------------------------|--------------|
| PUT /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}/<br>update-rules | vpc:firewalls:update   | -            |
| DELETE /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}               | vpc:firewalls:delete   | -            |
| GET /v3/<br>{project_id}/vpc/<br>firewalls                                    | vpc:firewalls:list     | -            |
| GET /v3/<br>{project_id}/vpc/<br>firewalls/<br>{firewall_id}                  | vpc:firewalls:get      | -            |
| POST /v2.0/<br>{project_id}/vpcs/<br>{vpc_id}/tags/action                     | vpc:vpcs:createTags    | -            |
| POST 01 /v2.0/<br>{project_id}/vpcs/<br>{vpc_id}/tags/action                  | vpc:vpcs:deleteTags    | -            |
| POST /v2.0/<br>{project_id}/vpcs/<br>{vpc_id}/tags                            | vpc:vpcs:createTags    | -            |
| POST /v2.0/<br>{project_id}/vpcs/<br>resource_instances/<br>action            | vpc:vpcs:listTags      | -            |
| GET /v2.0/<br>{project_id}/vpcs/<br>tags                                      | vpc:vpcs:listTags      | -            |
| GET /v2.0/<br>{project_id}/vpcs/<br>{vpc_id}/tags                             | vpc:vpcs:listTags      | -            |
| DELETE /v2.0/<br>{project_id}/vpcs/<br>{vpc_id}/tags/{key}                    | vpc:vpcs:deleteTags    | -            |
| POST 01 /v2.0/<br>{project_id}/<br>subnets/<br>{subnet_id}/tags/<br>action    | vpc:subnets:createTags | -            |

| API                                                                        | Action                          | Dependencies |
|----------------------------------------------------------------------------|---------------------------------|--------------|
| POST /v2.0/{project_id}/subnets/{subnet_id}/tags/action                    | vpc:subnets:deleteTags          | -            |
| POST /v2.0/{project_id}/subnets/{subnet_id}/tags                           | vpc:subnets:createTags          | -            |
| POST /v2.0/{project_id}/subnets/resource_instances/action                  | vpc:subnets:listTags            | -            |
| GET /v2.0/{project_id}/subnets/tags                                        | vpc:subnets:listTags            | -            |
| GET /v2.0/{project_id}/subnets/{subnet_id}/tags                            | vpc:subnets:listTags            | -            |
| DELETE /v2.0/{project_id}/subnets/{subnet_id}/tags/{key}                   | vpc:subnets:deleteTags          | -            |
| POST /v3/{project_id}/vpc/sub-network-interfaces                           | vpc:subNetworkInterfaces:create | -            |
| POST /v3/{project_id}/vpc/sub-network-interfaces/batch-create              | vpc:subNetworkInterfaces:create | -            |
| GET /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id} | vpc:subNetworkInterfaces:get    | -            |

| API                                                                           | Action                          | Dependencies |
|-------------------------------------------------------------------------------|---------------------------------|--------------|
| GET /v3/{project_id}/vpc/sub-network-interfaces                               | vpc:subNetworkInterfaces:list   | -            |
| GET /v3/{project_id}/vpc/sub-network-interfaces/count                         | vpc:subNetworkInterfaces:list   | -            |
| PUT /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id}    | vpc:subNetworkInterfaces:update | -            |
| DELETE /v3/{project_id}/vpc/sub-network-interfaces/{sub_network_interface_id} | vpc:subNetworkInterfaces:delete | -            |
| POST /v3/{project_id}/firewalls/{firewall_id}/tags/create                     | vpc:firewalls:createTags        | -            |
| POST /v3/{project_id}/firewalls/{firewall_id}/tags/delete                     | vpc:firewalls:deleteTags        | -            |
| POST /v3/{project_id}/firewalls/{firewall_id}/tags                            | vpc:firewalls:createTags        | -            |
| POST /v3/{project_id}/firewalls/resource-instances/filter                     | vpc:firewalls:listTags          | -            |
| POST /v3/{project_id}/firewalls/resource-instances/count                      | vpc:firewalls:listTags          | -            |

| API                                                                                        | Action                        | Dependencies |
|--------------------------------------------------------------------------------------------|-------------------------------|--------------|
| GET /v3/<br>{project_id}/<br>firewalls/tags                                                | vpc:firewalls:listTags        | -            |
| GET /v3/<br>{project_id}/<br>firewalls/<br>{firewall_id}/tags                              | vpc:firewalls:listTags        | -            |
| DELETE /v3/<br>{project_id}/<br>firewalls/<br>{firewall_id}/tags/<br>{tag_key}             | vpc:firewalls:deleteTags      | -            |
| POST 01 /v2.0/<br>{project_id}/<br>security-groups/<br>{security_group_id}/<br>tags/action | vpc:securityGroups:createTags | -            |
| POST /v2.0/<br>{project_id}/<br>security-groups/<br>{security_group_id}/<br>tags/action    | vpc:securityGroups:deleteTags | -            |
| POST /v2.0/<br>{project_id}/<br>security-groups/<br>{security_group_id}/<br>tags           | vpc:securityGroups:createTags | -            |
| POST /v2.0/<br>{project_id}/<br>security-groups/<br>resource_instances/<br>action          | vpc:securityGroups:listTags   | -            |
| GET /v2.0/<br>{project_id}/<br>security-groups/tags                                        | vpc:securityGroups:listTags   | -            |
| GET /v2.0/<br>{project_id}/<br>security-groups/<br>{security_group_id}/<br>tags            | vpc:securityGroups:listTags   | -            |

| API                                                                                  | Action                              | Dependencies |
|--------------------------------------------------------------------------------------|-------------------------------------|--------------|
| DELETE /v2.0/{project_id}/security-groups/{security_group_id}/tags/{key}             | vpc:securityGroups:deleteTags       | -            |
| POST /v3/{project_id}/vpc/traffic-mirror-filters                                     | vpc:trafficMirrorFilters:create     | -            |
| PUT /v3/{project_id}/vpc/traffic-mirror-filter/{traffic_mirror_filter_id}            | vpc:trafficMirrorFilters:update     | -            |
| GET /v3/{project_id}/vpc/traffic-mirror-filter/{traffic_mirror_filter_id}            | vpc:trafficMirrorFilters:get        | -            |
| GET /v3/{project_id}/vpc/traffic-mirror-filters                                      | vpc:trafficMirrorFilters:list       | -            |
| DELETE /v3/{project_id}/vpc/traffic-mirror-filter/{traffic_mirror_filter_id}         | vpc:trafficMirrorFilters:delete     | -            |
| POST /v3/{project_id}/vpc/traffic-mirror-filter-rules                                | vpc:trafficMirrorFilterRules:create | -            |
| PUT /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id} | vpc:trafficMirrorFilterRules:update | -            |
| GET /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id} | vpc:trafficMirrorFilterRules:get    | -            |



| API                                                                                         | Action                                 | Dependencies |
|---------------------------------------------------------------------------------------------|----------------------------------------|--------------|
| GET /v3/{project_id}/vpc/traffic-mirror-filter-rules                                        | vpc:trafficMirrorFilter-Rules:list     | -            |
| DELETE /v3/{project_id}/vpc/traffic-mirror-filter-rules/{traffic_mirror_filter_rule_id}     | vpc:trafficMirrorFilter-Rules:delete   | -            |
| POST /v3/{project_id}/vpc/traffic-mirror-sessions                                           | vpc:trafficMirrorSessions:create       | -            |
| PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/add-sources    | vpc:trafficMirrorSessions:addSource    | -            |
| PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}/remove-sources | vpc:trafficMirrorSessions:removeSource | -            |
| PUT /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}                | vpc:trafficMirrorSessions:update       | -            |
| GET /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id}                | vpc:trafficMirrorSessions:get          | -            |
| GET /v3/{project_id}/vpc/traffic-mirror-sessions                                            | vpc:trafficMirrorSessions:list         | -            |

| API                                                                             | Action                           | Dependencies |
|---------------------------------------------------------------------------------|----------------------------------|--------------|
| DELETE /v3/{project_id}/vpc/traffic-mirror-sessions/{traffic_mirror_session_id} | vpc:trafficMirrorSessions:delete | -            |
| PUT /v3/{project_id}/ports/{port_id}/insert-security-groups                     | vpc:ports:update                 | -            |
| PUT /v3/{project_id}/ports/{port_id}/remove-security-groups                     | vpc:ports:update                 | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-45](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for vpc.

**Table 3-45** Resource types supported by vpc

| Resource Type       | URN                                                                      |
|---------------------|--------------------------------------------------------------------------|
| network             | vpc:<region>:<account-id>:network:<network-id>                           |
| securityGroupRule   | vpc:<region>:<account-id>:securityGroupRule:<security-group-rule-id>     |
| addressGroup        | vpc:<region>:<account-id>:addressGroup:<address-group-id>                |
| firewall            | vpc:<region>:<account-id>:firewall:<firewall-id>                         |
| port                | vpc:<region>:<account-id>:port:<port-id>                                 |
| trafficMirrorFilter | vpc:<region>:<account-id>:trafficMirrorFilter:<traffic-mirror-filter-id> |
| securityGroup       | vpc:<region>:<account-id>:securityGroup:<security-group-id>              |

| Resource Type           | URN                                                                               |
|-------------------------|-----------------------------------------------------------------------------------|
| routeTable              | vpc:<region>:<account-id>:routeTable:<route-table-id>                             |
| vpc                     | vpc:<region>:<account-id>:vpc:<vpc-id>                                            |
| publicip                | vpc:<region>:<account-id>:publicip:<publicip-id>                                  |
| flowLog                 | vpc:<region>:<account-id>:flowLog:<flow-log-id>                                   |
| trafficMirrorFilterRule | vpc:<region>:<account-id>:trafficMirrorFilterRule:<traffic-mirror-filter-rule-id> |
| bandwidth               | vpc:<region>:<account-id>:bandwidth:<bandwidth-id>                                |
| trafficMirrorSession    | vpc:<region>:<account-id>:trafficMirrorSession:<traffic-mirror-session-id>        |
| subNetworkInterface     | vpc:<region>:<account-id>:subNetworkInterface:<sub-network-interface-id>          |
| subnet                  | vpc:<region>:<account-id>:subnet:<subnet-id>                                      |
| privatelp               | vpc:<region>:<account-id>:privatelp:<private-ip-id>                               |
| peering                 | vpc:<region>:<account-id>:peering:<peering-id>                                    |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, vpc) apply only to operations of the xx service. For details, see [Table 3-46](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when

its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by vpc

The following table lists the condition keys that you can define in identity policies for vpc. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-46** Service-specific condition keys supported by vpc

| Service-specific Condition Key    | Type   | Single-valued/<br>Multivalued | Description                                                                                          |
|-----------------------------------|--------|-------------------------------|------------------------------------------------------------------------------------------------------|
| vpc:VpcId                         | string | Multivalued                   | Filters access based on the specified vpc id.                                                        |
| vpc:VpcBlockServiceEndpointStates | string | Single-valued                 | Filters access based on the specified vpc block service endpoint, valid values should be on and off. |
| vpc:SubnetId                      | string | Multivalued                   | Filters access based on the specified subnet id.                                                     |
| vpc:SecurityGroupId               | string | Multivalued                   | Filters access based on the specified securityGroup id.                                              |
| vpc:PeeringId                     | string | Multivalued                   | Filters access based on the specified peering id.                                                    |
| vpc:AccepterVpcId                 | string | Multivalued                   | Filters access based on the specified accepter vpc id.                                               |
| vpc:AccepterVpcOrgPath            | string | Multivalued                   | Filters access based on the org path of specified accepter vpc owner.                                |
| vpc:AccepterVpcOwner              | string | Multivalued                   | Filters access based on the specified accepter vpc owner.                                            |
| vpc:RequesterVpcOrgPath           | string | Multivalued                   | Filters access based on the org path of specified requester vpc owner.                               |

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                                         |
|--------------------------------|--------|-------------------------------|---------------------------------------------------------------------------------------------------------------------|
| vpc:RequesterVpcOwner          | string | Multivalued                   | Filters access based on the specified requester vpc owner.                                                          |
| vpc:RequesterVpcId             | string | Multivalued                   | Filters access based on the specified requester vpc id.                                                             |
| vpc:RouteTableId               | string | Multivalued                   | Filters access based on the specified routeTable id.                                                                |
| vpc:FlowLogId                  | string | Multivalued                   | Filters access based on the specified flowLog id.                                                                   |
| vpc:AddressGroupId             | string | Multivalued                   | Filters access based on the specified addressGroup id.                                                              |
| vpc:FirewallId                 | string | Multivalued                   | Filters access based on the specified firewall id.                                                                  |
| vpc:PrivateIpId                | string | Multivalued                   | Filters access based on the specified privateIp id.                                                                 |
| vpc:PortId                     | string | Multivalued                   | Filters access based on the specified port id.                                                                      |
| vpc:SubNetworkInterfaceId      | string | Multivalued                   | Filters access based on the specified subNetworkInterface id.                                                       |
| vpc:FirewallRuleDirection      | string | Multivalued                   | Filters access based on the specified firewallRule direction, valid values should be ingress and egress.            |
| vpc:FirewallRuleProtocol       | string | Multivalued                   | Filters access based on the specified firewallRule protocol, valid values should be tcp, udp, icmp, icmpv6 and any. |

| Service-specific Condition Key  | Type    | Single-valued/<br>Multivalued | Description                                                                                                                                                                  |
|---------------------------------|---------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vpc:FirewallRuleAction          | string  | Multivalued                   | Filters access based on the specified firewallRule action, valid values should be allow and deny.                                                                            |
| vpc:FirewallRuleSourcePort      | numeric | Multivalued                   | Filters access based on the specified firewallRule source port.                                                                                                              |
| vpc:FirewallRuleDestinationPort | numeric | Multivalued                   | Filters access based on the specified firewallRule destination port.                                                                                                         |
| vpc:FirewallOperation-Type      | string  | Multivalued                   | Filters access based on the specified firewall operation type, valid values should be updateAcl, associateSubnet, disassociateSubnet, insertRule, updateRule and removeRule. |
| vpc:TrafficMirrorFilter-Id      | string  | Multivalued                   | Filters access based on the specified traffic mirror filter id.                                                                                                              |
| vpc:TrafficMirrorTargetType     | string  | Multivalued                   | Filters access based on the specified traffic mirror session target resource type, valid values should be eni and elb.                                                       |
| vpc:TrafficMirrorTargetId       | string  | Multivalued                   | Filters access based on the specified traffic mirror session target resource id.                                                                                             |
| vpc:TrafficMirrorSourceType     | string  | Multivalued                   | Filters access based on the specified traffic mirror session source resource type, valid values should be eni.                                                               |

| Service-specific Condition Key            | Type       | Single-valued/<br>Multivalued | Description                                                                                                                      |
|-------------------------------------------|------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| vpc:TrafficMirrorSourceId                 | string     | Multivalued                   | Filters access based on the specified traffic mirror session source resource id.                                                 |
| vpc:FirewallRuleSourceIp                  | ip_address | Single-valued                 | Filters access based on the source address in the specified network ACL rule.                                                    |
| vpc:FirewallRuleSourceIpAddressGroup      | string     | Single-valued                 | Filters access based on the unique ID of the IP address group used by the source address in the specified network ACL rule.      |
| vpc:FirewallRuleDestinationIp             | ip_address | Single-valued                 | Filters access based on the destination address in the specified network ACL rule.                                               |
| vpc:FirewallRuleDestinationIpAddressGroup | string     | Single-valued                 | Filters access based on the unique ID of the IP address group used by the destination address in the specified network ACL rule. |
| vpc:AvailabilityZone                      | string     | Single-valued                 | Filters access based on the specified AvailabilityZone.                                                                          |
| vpc:LegacyAPIFlavor                       | string     | Single-valued                 | Filters access based on the native api.                                                                                          |
| vpc:SecurityGroupRuleDirection            | string     | Single-valued                 | Filters access based on the specified securityGroupRule direction, valid values should be ingress and egress.                    |

| Service-specific Condition Key            | Type       | Single-valued/<br>Multivalued | Description                                                                                                                          |
|-------------------------------------------|------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| vpc:SecurityGroupRuleProtocol             | string     | Single-valued                 | Filters access based on the specified securityGroupRule protocol, valid values should be tcp, udp, icmp, icmpv6, gre and any.        |
| vpc:SecurityGroupRuleAction               | string     | Single-valued                 | Filters access based on the specified securityGroupRule action, valid values should be allow and deny.                               |
| vpc:SecurityGroupRulePort                 | numeric    | Multivalued                   | Filters access based on the specified securityGroupRule port.                                                                        |
| vpc:SecurityGroupRuleRemoteIpAddressGroup | string     | Single-valued                 | Filters access based on the unique ID of the IP address group used by the remote address group in the specified security group rule. |
| vpc:SecurityGroupRuleRemoteSecurityGroup  | string     | Single-valued                 | Filters access based on the unique security group ID used by the remote security group in the specified security group rule.         |
| vpc:SecurityGroupRuleRemoteIpPrefix       | ip_address | Single-valued                 | Filters access based on the IP address used by the remote IP address in the specified security group rule.                           |
| vpc:VirusubnetCidrReservationId           | string     | Multivalued                   | Filters access based on the specified virusubnetCidrReservation id.                                                                  |
| vpc:SubnetIpv6Enable                      | boolean    | Single-valued                 | Filters access based on the IPv6 enabling status of the specified subnet.                                                            |



### 3.3.3 Elastic IP

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by EIP, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.

- If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
- If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by EIP, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for EIP.

**Table 3-47** Actions supported by EIP

| Action                   | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|--------------------------|-----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| eip:publicips:createTags | Grants permission to create a tag for an EIP.       | Tagging      | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicipTags:create |
|                          |                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                         |
| eip:publicips:listTags   | Grants permission to query tags of a specified EIP. | List         | public ip *                 | -                                                                                                                                                  | vpc:publicipTags:get    |
| eip:publicips:deleteTags | Grants permission to delete an EIP tag.             | Tagging      | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicipTags:delete |
|                          |                                                     |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |                         |
| eip:publicips:count      | Grants permission to count EIPs.                    | List         | public ip *                 | -                                                                                                                                                  | vpc:publicips:list      |

| Action                     | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                | Alias                 |
|----------------------------|---------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| eip:bandwidths:create      | Grants permission to create shared bandwidth.                       | Write        | bandwidth*                  | -                                                                                                                            | vpc:bandwidths:create |
|                            |                                                                     |              | -                           | <b>g:EnterpriseProjectId</b>                                                                                                 |                       |
| eip:bandwidths:batchCreate | Grants permission to batch assign shared bandwidth.                 | Write        | bandwidth*                  | -                                                                                                                            | -                     |
| eip:bandwidths:list        | Grants permission to query shared bandwidths using search criteria. | List         | bandwidth*                  | -                                                                                                                            | vpc:bandwidths:list   |
|                            |                                                                     |              | -                           | <b>g:EnterpriseProjectId</b>                                                                                                 |                       |
| eip:bandwidths:update      | Grants permission to update information about shared bandwidth.     | Write        | bandwidth*                  | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul> | vpc:bandwidths:update |
| eip:bandwidths:get         | Grants permission to query details about a shared bandwidth.        | Read         | bandwidth*                  | <ul style="list-style-type: none"> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> <li><b>g:EnterpriseProjectId</b></li> </ul> | vpc:bandwidths:get    |
| eip:bandwidths:delete      | Grants permission to delete shared bandwidth.                       | Write        | bandwidth*                  | <ul style="list-style-type: none"> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> <li><b>g:EnterpriseProjectId</b></li> </ul> | vpc:bandwidths:delete |

| Action                    | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                    | Alias                 |
|---------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| eip:bandwidth Pkgs:list   | Grants permission to query bandwidth add-on packages using search criteria. | List         | bandwidth Pkg *             | -                                                                                                                                                                                | vpc:bandwidths:get    |
| eip:bandwidth Pkgs:update | Grants permission to update information about bandwidth add-on package.     | Write        | bandwidth Pkg *             | -                                                                                                                                                                                | vpc:bandwidths:update |
| eip:publicips:create      | Grants permission to assign EIP.                                            | Write        | public ip *                 | -                                                                                                                                                                                | vpc:publicips:create  |
|                           |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            |                       |
| eip:publicips:batchCreate | Grants permission to batch assign EIPs.                                     | Write        | public ip *                 | -                                                                                                                                                                                | vpc:publicips:create  |
|                           |                                                                             |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                       |
| eip:publicips:list        | Grants permission to query EIPs.                                            | List         | public ip *                 | -                                                                                                                                                                                | vpc:publicips:list    |
|                           |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            |                       |
| eip:publicips:get         | Grants permission to query a specific EIP.                                  | Read         | public ip *                 | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                   | vpc:publicips:get     |

| Action                             | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                |
|------------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| eip:publicips:update               | Grants permission to update an EIP.                        | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | vpc:publicips:update |
| eip:publicips:disassociateInstance | Grants permission to disassociate an instance from an EIP. | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | vpc:publicips:update |
| eip:publicips:delete               | Grants permission to release an EIP.                       | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | vpc:publicips:delete |
| eip:publicips:create               | Grants permission to assign EIP.                           | Write        | public ip *                 | -                                                                                                                                                                                      | vpc:publicips:create |
|                                    |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |                      |
| eip:publicips:batchCreate          | Grants permission to batch assign EIPs.                    | Write        | public ip *                 | -                                                                                                                                                                                      | vpc:publicips:create |
|                                    |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                      |
| eip:publicips:list                 | Grants permission to query EIPs.                           | List         | public ip *                 | -                                                                                                                                                                                      | vpc:publicips:list   |
|                                    |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |                      |
| eip:publicips:count                | Grants permission to count EIPs.                           | List         | public ip *                 | -                                                                                                                                                                                      | vpc:publicips:list   |

| Action                             | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                |
|------------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| eip:publicips:get                  | Grants permission to query a specific EIP.                 | Read         | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | vpc:publicips:get    |
| eip:publicips:update               | Grants permission to update an EIP.                        | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicips:update |
| eip:publicips:enableNat64          | Grants permission to enable nat64 of EIP.                  | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicips:update |
| eip:publicips:disableNat64         | Grants permission to enable nat64 of an EIP.               | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicips:update |
| eip:publicips:associateInstance    | Grants permission to associate an instance on an EIP.      | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicips:update |
| eip:publicips:disassociateInstance | Grants permission to disassociate an instance from an EIP. | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicips:update |

| Action                        | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|-------------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| eip:publicips:attachBandwidth | Grants permission to attach an EIP to a share bandwidth. | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicips:update    |
|                               |                                                          |              | bandwidth *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                         |
| eip:publicips:detachBandwidth | Grants permission to detach an EIP from share bandwidth. | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicips:update    |
|                               |                                                          |              | bandwidth *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                         |
| eip:publicips:delete          | Grants permission to release an EIP.                     | Write        | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | vpc:publicips:delete    |
| eip:publicips:createTags      | Grants permission to create a tag for an EIP.            | Tagging      | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicipTags:create |

| Action                         | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                    |
|--------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                                |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                          |
| eip:publicIps:listTags         | Grants permission to query tags of a specified EIP.         | List         | public ip *                 | -                                                                                                                                                  | vpc:publicIpsTags:get    |
| eip:publicIps:deleteTags       | Grants permission to delete an EIP tag.                     | Tagging      | public ip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:publicIpsTags:delete |
|                                |                                                             |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |                          |
| eip:bandwidths:insertPublicIps | Grants permission to add an EIP to a shared bandwidth.      | Write        | bandwidth *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | vpc:publicIps:insert     |
| eip:bandwidths:removePublicIps | Grants permission to remove an EIP from a shared bandwidth. | Write        | bandwidth *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | vpc:publicIps:insert     |
| eip:bandwidths:create          | Grants permission to create shared bandwidth.               | Write        | bandwidth *                 | -                                                                                                                                                  | vpc:bandwidths:create    |
|                                |                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                          |
| eip:bandwidths:batchCreate     | Grants permission to batch assign shared bandwidth.         | Write        | bandwidth *                 | -                                                                                                                                                  | -                        |



| Action                  | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                 |
|-------------------------|---------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| eip:bandwidths:list     | Grants permission to query shared bandwidths using search criteria. | List         | band width *                | -                                                                                                                                              | vpc:bandwidths:list   |
|                         |                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                       |
| eip:bandwidths:update   | Grants permission to update information about shared bandwidth.     | Write        | band width *                | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:bandwidths:update |
| eip:bandwidths:get      | Grants permission to query details about a shared bandwidth.        | Read         | band width *                | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | vpc:bandwidths:get    |
| eip:bandwidths:delete   | Grants permission to delete shared bandwidth.                       | Write        | band width *                | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | vpc:bandwidths:delete |
| eip:bandwidthRules:list | Grants permission to query bandwidth rules using search criteria.   | List         | band width *                | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:bandwidths:get    |
|                         |                                                                     |              | band width Rule *           | -                                                                                                                                              |                       |
| eip:bandwidthRules:get  | Grants permission to query details about a bandwidth rule.          | Read         | band width *                | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:bandwidths:get    |

| Action                     | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|----------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                            |                                                                             |              | bandwidth Rule *            | -                                                                                                                                                  |                       |
| eip:bandwidth Rules:update | Grants permission to update information about a bandwidth rule.             | Write        | bandwidth *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:bandwidths:update |
|                            |                                                                             |              | bandwidth Rule *            | -                                                                                                                                                  |                       |
| eip:bandwidth Rules:delete | Grants permission to delete bandwidth rule.                                 | Write        | bandwidth *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:bandwidths:delete |
|                            |                                                                             |              | bandwidth Rule *            | -                                                                                                                                                  |                       |
| eip:bandwidth Rules:create | Grants permission to create a bandwidth rule.                               | Write        | bandwidth *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | vpc:bandwidths:update |
|                            |                                                                             |              | bandwidth Rule *            | -                                                                                                                                                  |                       |
| eip:bandwidth Pkgs:list    | Grants permission to query bandwidth add-on packages using search criteria. | List         | bandwidth Pkg *             | -                                                                                                                                                  | vpc:bandwidths:get    |

| Action                   | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                | Alias                 |
|--------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|------------------------------|-----------------------|
| eip:bandwidthPkgs:get    | Grants permission to query details about a bandwidth add-on package.    | Read         | bandwidth Pkg *             | -                            | vpc:bandwidths:get    |
| eip:bandwidthPkgs:update | Grants permission to update information about bandwidth add-on package. | Write        | bandwidth Pkg *             | -                            | vpc:bandwidths:update |
| eip:bandwidthPkgs:create | Grants permission to create a bandwidth add-on package.                 | Write        | bandwidth Pkg *             | -                            | vpc:bandwidths:update |
| eip:publicipPools:create | Grants permission to create an EIP pool.                                | Write        | publicipPool *              | -                            | vpc:publicips:create  |
| eip:publicipPools:update | Grants permission to update information about EIP pool.                 | Write        | publicipPool *              | -                            | vpc:publicips:update  |
| eip:globalEips:list      | Grants permission to query global elastic IPs.                          | List         | globalEip *                 | -                            | -                     |
|                          |                                                                         |              | -                           | <b>g:EnterpriseProjectId</b> |                       |
| eip:globalEips:count     | Grants permission to count global elastic IPs.                          | List         | globalEip *                 | -                            | eip:globalEips:list   |

| Action                              | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                 |
|-------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| eip:globalEips:get                  | Grants permission to query a specific global elastic IP.                | Read         | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -                     |
| eip:globalEips:create               | Grants permission to assign global elastic IP.                          | Write        | globalEip *                 | -                                                                                                                                                                                      | -                     |
|                                     |                                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                       |
| eip:globalEips:updateGeip           | Grants permission to update a global elastic IP.                        | Write        | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | eip:globalEips:update |
| eip:globalEips:disassociateInstance | Grants permission to disassociate an instance from a global elastic IP. | Write        | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | eip:globalEips:update |
| eip:globalEips:associateInstance    | Grants permission to associate an instance on a global elastic IP.      | Write        | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | eip:globalEips:update |
| eip:globalEips:delete               | Grants permission to release a global elastic IP.                       | Write        | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -                     |

| Action                         | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|--------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| eip:globalEips:attachBandwidth | Grants permission to attach a global elastic IP to a global internet bandwidth.   | Write        | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | eip:globalEips:insert |
|                                |                                                                                   |              | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                       |
| eip:globalEips:detachBandwidth | Grants permission to detach a global elastic IP from a global internet bandwidth. | Write        | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | eip:globalEips:remove |
|                                |                                                                                   |              | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                       |
| eip:globalEips:createTags      | Grants permission to create a tag for a global elastic IP.                        | Tagging      | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                     |
|                                |                                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                       |

| Action                            | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| eip:globalEips:getTags            | Grants permission to query tags of a specified global elastic IP.         | Read         | globalEip *                 | -                                                                                                                                                  | -     |
| eip:globalEips:listTags           | Grants permission to list tags of global elastic IPs in project.          | List         | globalEip *                 | -                                                                                                                                                  | -     |
| eip:globalEips:deleteTags         | Grants permission to delete a global elastic IP tag.                      | Tagging      | globalEip *                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                   |                                                                           |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |       |
| eip:internetBandwidths:createTags | Grants permission to create a tag for a global internet bandwidth.        | Tagging      | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                   |                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| eip:internetBandwidths:getTags    | Grants permission to query tags of a specified global internet bandwidth. | Read         | internetBandwidth *         | -                                                                                                                                                  | -     |

| Action                            | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                       |
|-----------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| eip:internetBandwidths:listTags   | Grants permission to list tags of global internet bandwidths in project. | List         | internetBandwidth *         | -                                                                                                                                                  | -                           |
| eip:internetBandwidths:deleteTags | Grants permission to delete a global internet bandwidth tag.             | Tagging      | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                           |
|                                   |                                                                          |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |                             |
| eip:internetBandwidths:list       | Grants permission to query global internet bandwidths.                   | List         | internetBandwidth *         | -                                                                                                                                                  | -                           |
|                                   |                                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                             |
| eip:internetBandwidths:count      | Grants permission to count global internet bandwidths.                   | List         | internetBandwidth *         | -                                                                                                                                                  | eip:internetBandwidths:list |
| eip:internetBandwidths:get        | Grants permission to query a specific global internet bandwidth.         | Read         | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                           |
| eip:internetBandwidths:create     | Grants permission to create global internet bandwidth.                   | Write        | internetBandwidth *         | -                                                                                                                                                  | -                           |
|                                   |                                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                             |

| Action                        | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|-------------------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| eip:internetBandwidths:update | Grants permission to update a global internet bandwidth.         | Write        | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| eip:internetBandwidths:delete | Grants permission to delete global internet bandwidth.           | Write        | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| eip:geipSegments:list         | Grants permission to query global elastic IP segments.           | List         | geipSegment *               | -                                                                                                                                                                                      | -     |
|                               |                                                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| eip:geipSegments:count        | Grants permission to count global elastic IP segments.           | List         | geipSegment *               | -                                                                                                                                                                                      | -     |
| eip:geipSegments:get          | Grants permission to query a specific global elastic IP segment. | Read         | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -     |
| eip:geipSegments:create       | Grants permission to assign global elastic IP segment.           | Write        | geipSegment *               | -                                                                                                                                                                                      | -     |
|                               |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |



| Action                                | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| eip:geipSegments:update               | Grants permission to update a global elastic IP segment.                                | Write        | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| eip:geipSegments:disassociateInstance | Grants permission to disassociate an instance from a global elastic IP segment.         | Write        | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| eip:geipSegments:associateInstance    | Grants permission to associate an instance on a global elastic IP segment.              | Write        | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| eip:geipSegments:delete               | Grants permission to release a global elastic IP segment.                               | Write        | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| eip:geipSegments:attachBandwidth      | Grants permission to attach a global elastic IP segment to a global internet bandwidth. | Write        | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                       |                                                                                         |              | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |

| Action                           | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| eip:geipSegments:detachBandwidth | Grants permission to detach a global elastic IP segment from a global internet bandwidth. | Write        | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                  |                                                                                           |              | internetBandwidth *         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
| eip:geipSegments:createTags      | Grants permission to create a tag for a global elastic IP segment.                        | Tagging      | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                  |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| eip:geipSegments:getTags         | Grants permission to query tags of a specified global elastic IP segment.                 | Read         | geipSegment *               | -                                                                                                                                                  | -     |
| eip:geipSegments:listTags        | Grants permission to list tags of global elastic IP segments in project.                  | List         | geipSegment *               | -                                                                                                                                                  | -     |
| eip:geipSegments:deleteTags      | Grants permission to delete a global elastic IP segment tag.                              | Tagging      | geipSegment *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

| Action                    | Description                                           | Access Level | Resource Type (*: required) | Condition Key             | Alias |
|---------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------------------|-------|
|                           |                                                       |              | -                           | <a href="#">g:TagKeys</a> |       |
| eip:userDisclaimer:sign   | Grants permission to sign a user disclaimer record.   | Write        | -                           | -                         | -     |
| eip:userDisclaimer:cancel | Grants permission to cancel a user disclaimer record. | Write        | -                           | -                         | -     |

Each API of EIP usually supports one or more actions. [Table 3-48](#) lists the supported actions and dependencies.

**Table 3-48** Actions and dependencies supported by EIP APIs

| API                                                            | Action                   | Dependencies |
|----------------------------------------------------------------|--------------------------|--------------|
| GET /v2/{project_id}/elasticips                                | eip:publicips:count      | -            |
| GET /v2/{project_id}/publicip/instances                        | eip:publicips:count      | -            |
| POST /v2.0/{project_id}/publicips/{publicip_id}/tags/action    | eip:publicips:createTags | -            |
| POST 01 /v2.0/{project_id}/publicips/{publicip_id}/tags/action | eip:publicips:deleteTags | -            |
| POST /v2.0/{project_id}/publicips/{publicip_id}/tags           | eip:publicips:createTags | -            |

| API                                                                          | Action                     | Dependencies |
|------------------------------------------------------------------------------|----------------------------|--------------|
| DELETE /v2.0/<br>{project_id}/<br>publicips/<br>{publicip_id}/tags/<br>{key} | eip:publicips:deleteTags   | -            |
| POST /v2.0/<br>{project_id}/<br>publicips/<br>resource_instances/<br>action  | eip:publicips:listTags     | -            |
| GET /v2.0/<br>{project_id}/<br>publicips/tags                                | eip:publicips:listTags     | -            |
| GET /v2.0/<br>{project_id}/<br>publicips/<br>{publicip_id}/tags              | eip:publicips:listTags     | -            |
| POST /v2.0/<br>{project_id}/<br>bandwidths                                   | eip:bandwidths:create      | -            |
| POST /v2.0/<br>{project_id}/batch-<br>bandwidths                             | eip:bandwidths:batchCreate | -            |
| GET /v1/<br>{project_id}/<br>bandwidths                                      | eip:bandwidths:list        | -            |
| DELETE /v2.0/<br>{project_id}/<br>bandwidths/<br>{bandwidth_id}              | eip:bandwidths:delete      | -            |
| GET /v1/<br>{project_id}/<br>bandwidths/<br>{bandwidth_id}                   | eip:bandwidths:get         | -            |
| PUT /v1/<br>{project_id}/<br>bandwidths/<br>{bandwidth_id}                   | eip:bandwidths:update      | -            |
| PUT /v2.0/<br>{project_id}/<br>bandwidths/<br>{bandwidth_id}                 | eip:bandwidths:update      | -            |

| API                                                      | Action                         | Dependencies       |
|----------------------------------------------------------|--------------------------------|--------------------|
| POST /v2.0/{project_id}/bandwidths/change-to-period      | eip:bandwidths:update          | bss:renewal:update |
| GET /v2/{project_id}/bandwidthpkgs                       | eip:bandwidthPkgs:list         | -                  |
| PUT /v2/{project_id}/bandwidthpkgs/{id}                  | eip:bandwidthPkgs:update       | -                  |
| PUT /v2/{project_id}/batch-bandwidths/modify             | eip:bandwidths:update          | -                  |
| POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/insert | eip:bandwidths:insertPublicIps | -                  |
| POST /v2.0/{project_id}/bandwidths/{bandwidth_id}/remove | eip:bandwidths:removePublicIps | -                  |
| POST /v1/{project_id}/publicips                          | eip:publicIps:create           | -                  |
| POST /v2/{project_id}/batchpublicips                     | eip:publicIps:batchCreate      | -                  |
| GET /v1/{project_id}/publicips                           | eip:publicIps:list             | -                  |
| GET /v1/{project_id}/publicips/{publicip_id}             | eip:publicIps:get              | -                  |
| PUT /v1/{project_id}/publicips/{publicip_id}             | eip:publicIps:update           | -                  |

| API                                                                      | Action                             | Dependencies       |
|--------------------------------------------------------------------------|------------------------------------|--------------------|
| POST /v2.0/{project_id}/publicips/change-to-period                       | eip:publicips:update               | bss:renewal:update |
| PATCH /v2/{project_id}/batchpublicips                                    | eip:publicips:disassociateInstance | -                  |
| DELETE /v1/{project_id}/publicips/{publicip_id}                          | eip:publicips:delete               | -                  |
| DELETE /v2/{project_id}/batchpublicips                                   | eip:publicips:delete               | -                  |
| POST /v3/{project_id}/eip/publicips/{publicip_id}/associate-instance     | eip:publicips:associateInstance    | -                  |
| POST /v3/{project_id}/eip/publicips/{publicip_id}/disassociate-instance  | eip:publicips:disassociateInstance | -                  |
| POST /v3/{project_id}/eip/publicips/attach-share-bandwidth               | eip:publicips:attachBandwidth      | -                  |
| POST /v3/{project_id}/eip/publicips/{publicip_id}/attach-share-bandwidth | eip:publicips:attachBandwidth      | -                  |
| POST /v3/{project_id}/eip/publicips/detach-share-bandwidth               | eip:publicips:detachBandwidth      | -                  |
| POST /v3/{project_id}/eip/publicips/{publicip_id}/detach-share-bandwidth | eip:publicips:detachBandwidth      | -                  |

| API                                                                                       | Action                     | Dependencies |
|-------------------------------------------------------------------------------------------|----------------------------|--------------|
| POST /v3/{project_id}/eip/bandwidths                                                      | eip:bandwidths:create      | -            |
| GET /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rules                        | eip:bandwidthRules:list    | -            |
| GET /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rule/{bandwidth_rules_id}    | eip:bandwidthRules:get     | -            |
| PUT /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rule/{bandwidth_rules_id}    | eip:bandwidthRules:update  | -            |
| POST /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rules                       | eip:bandwidthRules:create  | -            |
| DELETE /v3/{project_id}/eip/bandwidths/{bandwidth_id}/bandwidth-rule/{bandwidth_rules_id} | eip:bandwidthRules:delete  | -            |
| POST /v3/{project_id}/eip/publicips/publicips/{publicip_id}/enable-nat64                  | eip:publicIps:enableNat64  | -            |
| POST /v3/{project_id}/eip/publicips/publicips/{publicip_id}/disable-nat64                 | eip:publicIps:disableNat64 | -            |

| API                                              | Action              | Dependencies |
|--------------------------------------------------|---------------------|--------------|
| GET /v3/{project_id}/eip-bandwidths              | eip:bandwidths:list | -            |
| GET /v3/{project_id}/eip/bandwidths              | eip:bandwidths:list | -            |
| GET /v3/{project_id}/eip/publicips               | eip:publicips:list  | -            |
| GET /v3/{project_id}/eip/publicips/{publicip_id} | eip:publicips:get   | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-49](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for EIP.

**Table 3-49** Resource types supported by EIP

| Resource Type     | URN                                                                |
|-------------------|--------------------------------------------------------------------|
| bandwidthRule     | eip:<region>:<account-id>:bandwidthRule:<bandwidthRule-id>         |
| bandwidth         | vpc:<region>:<account-id>:bandwidth:<bandwidth-id>                 |
| bandwidthPkg      | eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>           |
| publicipPool      | eip:<region>:<account-id>:publicipPool:<publicipPool-id>           |
| geipSegment       | eip:<region>:<account-id>:geipSegment:<geipSegment-id>             |
| vpclgw            | eip:<region>:<account-id>:vpclgw:<vpclgw-id>                       |
| internetBandwidth | eip:<region>:<account-id>:internetBandwidth:<internetBandwidth-id> |



| Resource Type | URN                                                |
|---------------|----------------------------------------------------|
| publicip      | vpc:<region>:<account-id>:publicip:<publicip-id>   |
| globalEip     | eip:<region>:<account-id>:globalEip:<globalEip-id> |

## Conditions

EIP does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.3.4 Direct Connect

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.

- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DC, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DC, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DC.

**Table 3-50** Actions supported by DC

| Action                     | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|----------------------------|-------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:directConnect:create | Grants permission to create a connection. | Write        | direct Connect *            | -                                                                                                                                                                                      |       |
|                            |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |       |
| dcaas:directConnect:update | Grants permission to update a connection. | Write        | direct Connect *            | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |

| Action                                        | Description                                                                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                        |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| dcaas:directConnect:delete                    | Grants permission to delete a pay-per-use connection. A yearly/monthly connection can only be unsubscribed from. | Write        | directConnect *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                            |
| dcaas:directConnect:get                       | Grants permission to query details of a connection.                                                              | Read         | directConnect *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                            |
| dcaas:directConnect:list                      | Grants permission to list the connections .                                                                      | List         | directConnect *             | -                                                                                                                                                  | -                            |
|                                               |                                                                                                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                              |
| dcaas:directConnect:createHostedDirectConnect | Grants permission to allow a partner to create a hosted connection.                                              | Write        | directConnect *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • dcaas:directConnect:create |
| dcaas:directConnect:updateHostedDirectConnect | Grants permission to allow a partner to update a hosted connection.                                              | Write        | directConnect *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • dcaas:directConnect:update |

| Action                                         | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                                                                          |
|------------------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| dcaas:directConnect:deleteHostedDirectConnect  | Grants permission to allow a partner to delete a hosted connection.           | Write        | directConnect *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dcaas:directConnect:delete</li> </ul> |
| dcaas:directConnect:getHostedDirectConnect     | Grants permission to allow a partner to query details of a hosted connection. | Read         | directConnect *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dcaas:directConnect:get</li> </ul>    |
| dcaas:directConnect:listHostedDirectConnect    | Grants permission to allow a partner to list the hosted connections.          | List         | directConnect *             | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dcaas:directConnect:list</li> </ul>   |
| dcaas:directConnect:createOnestopDirectConnect | Grants permission to create a full-service connection.                        | Write        | directConnect *             | -                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• dcaas:directConnect:create</li> </ul> |
|                                                |                                                                               |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                                |
| dcaas:directConnect:updateOnestopDirectConnect | Grants permission to update a full-service connection.                        | Write        | directConnect *             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dcaas:directConnect:update</li> </ul> |

| Action                          | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                    | Alias                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| dcaas:directConnect:createOrder | Grants permission to create an order for a connection.                                 | Write        | directConnect *             | -                                                                                                                                | <ul style="list-style-type: none"> <li>dcaas:directConnect:create</li> </ul> |
| dcaas:directConnect:updateOrder | Grants permission to modify the order for changing the specifications of a connection. | Write        | directConnect *             | -                                                                                                                                | <ul style="list-style-type: none"> <li>dcaas:directConnect:update</li> </ul> |
| dcaas:vgw:create                | Grants permission to create a virtual gateway.                                         | Write        | vgw *                       | -                                                                                                                                | -                                                                            |
|                                 |                                                                                        |              | vpc                         | -                                                                                                                                |                                                                              |
|                                 |                                                                                        |              | instances                   | -                                                                                                                                |                                                                              |
|                                 |                                                                                        |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |                                                                              |
| dcaas:vgw:update                | Grants permission to update a virtual gateway.                                         | Write        | vgw *                       | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>                   | -                                                                            |
| dcaas:vgw:delete                | Grants permission to delete a virtual gateway.                                         | Write        | vgw *                       | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>                   | -                                                                            |

| Action           | Description                                              | Access Level | Resource Type (*: required)                                                 | Condition Key                                                                                                                                                                                                             | Alias |
|------------------|----------------------------------------------------------|--------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:vgw:get    | Grants permission to query details of a virtual gateway. | Read         | vgw *                                                                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                        | -     |
| dcaas:vgw:list   | Grants permission to list the virtual gateways.          | List         | vgw *<br>-                                                                  | -<br><a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                | -     |
| dcaas:vif:create | Grants permission to create a virtual interface.         | Write        | vif *<br>direct Connect<br>lag<br>vgw<br>gdgw<br>connectGateway<br>lgw<br>- | -<br>-<br>-<br>-<br>-<br>-<br>-<br><ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -     |
| dcaas:vif:update | Grants permission to update a virtual interface.         | Write        | vif *                                                                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                        | -     |

| Action                             | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:vif:delete                   | Grants permission to delete a virtual interface.                        | Write        | vif *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:vif:get                      | Grants permission to query details of a virtual interface.              | Read         | vif *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:vif:list                     | Grants permission to list the virtual interfaces.                       | List         | vif *                       | -                                                                                                                                                  | -     |
|                                    |                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| dcaas:vif:updateVifExtendAttribute | Grants permission to update extended attributes of a virtual interface. | Write        | vif *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:vifPeer:create               | Grants permission to create a virtual interface peer.                   | Write        | vifPeer *                   | -                                                                                                                                                  | -     |
|                                    |                                                                         |              | vif *                       | -                                                                                                                                                  |       |
| dcaas:vifPeer:update               | Grants permission to update a virtual interface peer.                   | Write        | vifPeer *                   | -                                                                                                                                                  | -     |
| dcaas:vifPeer:delete               | Grants permission to delete a virtual interface peer.                   | Write        | vifPeer *                   | -                                                                                                                                                  | -     |

| Action             | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                         | Alias |
|--------------------|-----------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:vifPeer:get  | Grants permission to query details of a virtual interface peer. | Read         | vifPeer *                   | -                                                                                                                                                     | -     |
| dcaas:vifPeer:list | Grants permission to list the virtual interface peers.          | List         | vifPeer *                   | -                                                                                                                                                     | -     |
| dcaas:lag:list     | Grants permission to list the LAGs.                             | List         | lag *                       | -                                                                                                                                                     | -     |
|                    |                                                                 |              | -                           | <b>g:EnterpriseProjectId</b>                                                                                                                          |       |
| dcaas:gdgw:create  | Grants permission to create a global DC gateway.                | Write        | gdgw *                      | -                                                                                                                                                     | -     |
|                    |                                                                 |              | -                           | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:RequestTag/&lt;tag-key&gt;</b></li> <li><b>g:TagKeys</b></li> </ul> |       |
| dcaas:gdgw:update  | Grants permission to update a global DC gateway.                | Write        | gdgw *                      | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul>                          | -     |
| dcaas:gdgw:delete  | Grants permission to delete a global DC gateway.                | Write        | gdgw *                      | <ul style="list-style-type: none"> <li><b>g:EnterpriseProjectId</b></li> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul>                          | -     |



| Action                    | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:gdgw:get            | Grants permission to query details of a global DC gateway.                | Read         | gdgw*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:gdgw:list           | Grants permission to list the global DC gateways.                         | List         | gdgw*                       | -                                                                                                                                                  | -     |
|                           |                                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| dcaas:gdgw:createPeerlink | Grants permission to create a peer link for a global DC gateway.          | Write        | gdgw*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:gdgw:updatePeerlink | Grants permission to update a peer link of a global DC gateway.           | Write        | gdgw*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:gdgw:deletePeerlink | Grants permission to delete a peer link of a global DC gateway.           | Write        | gdgw*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:gdgw:getPeerlink    | Grants permission to query details of a peer link of a global DC gateway. | Read         | gdgw*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

| Action                             | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:gdgw:listPeerlink            | Grants permission to list the peer links of a global DC gateway.      | List         | gdgw*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:connectGateway:create        | Grants permission to create a connect gateway.                        | Write        | connectGateway*             | -                                                                                                                                                  | -     |
| dcaas:connectGateway:update        | Grants permission to update a connect gateway.                        | Write        | connectGateway*             | -                                                                                                                                                  | -     |
| dcaas:connectGateway:delete        | Grants permission to delete a connect gateway.                        | Write        | connectGateway*             | -                                                                                                                                                  | -     |
| dcaas:connectGateway:get           | Grants permission to query details of a connect gateway.              | Read         | connectGateway*             | -                                                                                                                                                  | -     |
| dcaas:connectGateway:list          | Grants permission to list the connect gateways.                       | List         | connectGateway*             | -                                                                                                                                                  | -     |
| dcaas:connectGateway:listGlobalEip | Grants permission to list the global EIPs bound to a connect gateway. | List         | connectGateway*             | -                                                                                                                                                  | -     |

| Action                               | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:connectGateway:bindGlobalEip   | Grants permission to bind a global EIP to a connect gateway.                | Write        | connectGateway *            | -                                                                                                                                                  | -     |
| dcaas:connectGateway:unbindGlobalEip | Grants permission to unbind a global EIP from a connect gateway.            | Write        | connectGateway *            | -                                                                                                                                                  | -     |
| dcaas:vif:switchoverTest             | Grants permission to perform a switchover test.                             | Write        | vif *                       | -                                                                                                                                                  | -     |
| dcaas:vif:listSwitchoverTestRecord   | Grants permission to query switchover test execution records.               | List         | vif *                       | -                                                                                                                                                  | -     |
| dcaas:vif:getSwitchoverTestRecord    | Grants permission to query a switchover test execution record.              | Read         | vif *                       | -                                                                                                                                                  | -     |
| dcaas:resources:batchTagUntag        | Grants permission to add tags to or delete tags from a resource in batches. | Tagging      | directConnect               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

| Action                          | Description                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------|------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                 |                                                |              | lag                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                                 |                                                |              | vgw                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                                 |                                                |              | vif                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                                 |                                                |              | gdgw                        | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                                 |                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| dcaas:resources:listResourceTag | Grants permission to query tags of a resource. | List         | direct Connect              | -                                                                                                                                                  | -     |
|                                 |                                                |              | lag                         | -                                                                                                                                                  |       |
|                                 |                                                |              | vgw                         | -                                                                                                                                                  |       |
|                                 |                                                |              | vif                         | -                                                                                                                                                  |       |
|                                 |                                                |              | gdgw                        | -                                                                                                                                                  |       |

| Action                  | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------|---------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:resources:listTag | Grants permission to query tags by resource type. | List         | direct Connect              | -                                                                                                                                                  | -     |
|                         |                                                   |              | lag                         | -                                                                                                                                                  |       |
|                         |                                                   |              | vgw                         | -                                                                                                                                                  |       |
|                         |                                                   |              | vif                         | -                                                                                                                                                  |       |
|                         |                                                   |              | gdgw                        | -                                                                                                                                                  |       |
| dcaas:resources:tag     | Grants permission to add a tag to a resource.     | Tagging      | direct Connect              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                         |                                                   |              | lag                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                         |                                                   |              | vgw                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                         |                                                   |              | vif                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                         |                                                   |              | gdgw                        | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |

| Action                | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                       |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| dcaas:resources:unTag | Grants permission to delete a tag from a resource. | Tagging      | direct Connect              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                       |                                                    |              | lag                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                       |                                                    |              | vgw                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                       |                                                    |              | vif                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                       |                                                    |              | gdgw                        | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
|                       |                                                    |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |       |

| Action                          | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcaas:resources:listByTag       | Grants permission to query resources by tag.                                           | List         | direct Connect              | -                                                                                                                                                  | -     |
|                                 |                                                                                        |              | lag                         | -                                                                                                                                                  |       |
|                                 |                                                                                        |              | vgw                         | -                                                                                                                                                  |       |
|                                 |                                                                                        |              | vif                         | -                                                                                                                                                  |       |
|                                 |                                                                                        |              | gdgw                        | -                                                                                                                                                  |       |
| dcaas:gdgw:listGdgwRouteTable   | Grants permission to obtain the routing table of the Direct Connect global dc gateway. | List         | gdgw *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:gdgw:updateGdgwRouteTable | Grants permission to update the routing table of the Direct Connect global dc gateway. | Write        | gdgw *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:vgw:listVgwRouteTable     | Grants permission to obtain the routing table of the Direct Connect virtual gateway.   | List         | vgw *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| dcaas:vgw:updateVgwRouteTable   | Grants permission to update the routing table of the Direct Connect virtual gateway.   | Write        | vgw *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

| Action                   | Description                                                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------|---------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dcaas:quota:listVgwUsage | Grants permission to query the quota of VPCs that a virtual gateway can be associated with. | List         | -                           | -             | -     |
| dcaas:quota:listUsage    | Grants permission to query the quotas.                                                      | List         | -                           | -             | -     |
| dcaas:lgw:create         | Grants permission to create a local gateway.                                                | Write        | lgw *                       | -             | -     |
| dcaas:lgw:update         | Grants permission to update a local gateway.                                                | Write        | lgw *                       | -             | -     |
| dcaas:lgw:delete         | Grants permission to delete a local gateway.                                                | Write        | lgw *                       | -             | -     |
| dcaas:lgw:get            | Grants permission to query details of a local gateway.                                      | Read         | lgw *                       | -             | -     |
| dcaas:lgw:list           | Grants permission to list the local gateways.                                               | List         | lgw *                       | -             | -     |
| dcaas:lgwTable:create    | Grants permission to create a local gateway route table.                                    | Write        | lgwTable *                  | -             | -     |
|                          |                                                                                             |              | lgw *                       | -             |       |



| Action                             | Description                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dcaas:lgwTable:update              | Grants permission to update a local gateway route table.              | Write        | lgwTable *                  | -             | -     |
| dcaas:lgwTable:delete              | Grants permission to delete a local gateway route table.              | Write        | lgwTable *                  | -             | -     |
| dcaas:lgwTable:get                 | Grants permission to query details of a local gateway route table.    | Read         | lgwTable *                  | -             | -     |
| dcaas:lgwTable:list                | Grants permission to list the local gateway route tables.             | List         | lgwTable *                  | -             | -     |
| dcaas:lgwTable:createLgwTableRoute | Grants permission to create a route in a local gateway route table.   | Write        | lgwTable *                  | -             | -     |
| dcaas:lgwTable:updateLgwTableRoute | Grants permission to update a route in a local gateway route table.   | Write        | lgwTable *                  | -             | -     |
| dcaas:lgwTable:deleteLgwTableRoute | Grants permission to delete a route from a local gateway route table. | Write        | lgwTable *                  | -             | -     |

| Action                                  | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dcaas:lgwTable:getLgwTableRoute         | Grants permission to query details of a route in a local gateway route table.   | Read         | lgwTable *                  | -             | -     |
| dcaas:lgwTable:listLgwTableRoute        | Grants permission to list the routes in a local gateway route table.            | List         | lgwTable *                  | -             | -     |
| dcaas:lgwTable:batchDeleteLgwTableRoute | Grants permission to delete routes from a local gateway route table in batches. | Write        | lgwTable *                  | -             | -     |
| dcaas:lgwTable:createLgwTableVpc        | Grants permission to associate a local gateway route table with a VPC.          | Write        | lgwTable *                  | -             | -     |
|                                         |                                                                                 |              | vpc *                       | -             |       |
| dcaas:lgwTable:updateLgwTableVpc        | Grants permission to update a VPC for a local gateway route table.              | Write        | lgwTable *                  | -             | -     |
| dcaas:lgwTable:deleteLgwTableVpc        | Grants permission to disassociate a local gateway route table from a VPC.       | Write        | lgwTable *                  | -             | -     |

| Action                         | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dcaas:lgwTable:getLgwTableVpc  | Grants permission to query details of a VPC that a local gateway route table is associated with. | Read         | lgwTable *                  | -             | -     |
| dcaas:lgwTable:listLgwTableVpc | Grants permission to list the VPCs that a local gateway route table is associated with.          | List         | lgwTable *                  | -             | -     |

Each API of DC usually supports one or more actions. [Table 3-51](#) lists the supported actions and dependencies.

**Table 3-51** Actions and dependencies supported by DC APIs

| API                                                               | Action                     | Dependencies |
|-------------------------------------------------------------------|----------------------------|--------------|
| GET /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}    | dcaas:directConnect:get    | -            |
| GET /v3/{project_id}/dcaas/direct-connects                        | dcaas:directConnect:list   | -            |
| PUT /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}    | dcaas:directConnect:update | -            |
| DELETE /v3/{project_id}/dcaas/direct-connects/{direct_connect_id} | dcaas:directConnect:delete | -            |

| API                                                                  | Action                                        | Dependencies                                                                                 |
|----------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------|
| GET /v3/{project_id}/dcaas/hosted-connects                           | dcaas:directConnect:listHostedDirectConnect   | -                                                                                            |
| POST /v3/{project_id}/dcaas/hosted-connects                          | dcaas:directConnect:createHostedDirectConnect | -                                                                                            |
| PUT /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}       | dcaas:directConnect:updateHostedDirectConnect | -                                                                                            |
| DELETE /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}    | dcaas:directConnect:deleteHostedDirectConnect | -                                                                                            |
| GET /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}     | dcaas:vgw:get                                 | -                                                                                            |
| GET /v3/{project_id}/dcaas/virtual-gateways                          | dcaas:vgw:list                                | -                                                                                            |
| PUT /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}     | dcaas:vgw:update                              | -                                                                                            |
| DELETE /v3/{project_id}/dcaas/virtual-gateways/{virtual_gateway_id}  | dcaas:vgw:delete                              | -                                                                                            |
| POST /v3/{project_id}/dcaas/virtual-gateways                         | dcaas:vgw:create                              | <ul style="list-style-type: none"> <li>• er:instances:get</li> <li>• vpc:vpcs:get</li> </ul> |
| GET /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id} | dcaas:vif:get                                 | -                                                                                            |
| GET /v3/{project_id}/dcaas/virtual-interfaces                        | dcaas:vif:list                                | -                                                                                            |

| API                                                                                            | Action                             | Dependencies |
|------------------------------------------------------------------------------------------------|------------------------------------|--------------|
| PUT /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}                           | dcaas:vif:update                   | -            |
| DELETE /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}                        | dcaas:vif:delete                   | -            |
| POST /v3/{project_id}/dcaas/virtual-interfaces                                                 | dcaas:vif:create                   | -            |
| PUT /v3/{project_id}/dcaas/vif-peers/{vif_peer_id}                                             | dcaas:vifPeer:update               | -            |
| DELETE /v3/{project_id}/dcaas/vif-peers/{vif_peer_id}                                          | dcaas:vifPeer:delete               | -            |
| POST /v3/{project_id}/dcaas/vif-peers                                                          | dcaas:vifPeer:create               | -            |
| GET /v3/{project_id}/dcaas/global-dc-gateways/{global_dc_gateway_id}                           | dcaas:gdgw:get                     | -            |
| GET /v3/{project_id}/dcaas/global-dc-gateways/{global_dc_gateway_id}/peer-links/{peer_link_id} | dcaas:gdgw:getPeerlink             | -            |
| POST /v3/{project_id}/dcaas/switchover-test                                                    | dcaas:vif:switchoverTest           | -            |
| GET /v3/{project_id}/dcaas/switchover-test                                                     | dcaas:vif:listSwitchoverTestRecord | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-52](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DC.

**Table 3-52** Resource types supported by DC

| Resource Type  | URN                                                            |
|----------------|----------------------------------------------------------------|
| instances      | er:<region>:<account-id>:instances:<instance-id>               |
| lgw            | dcaas:<region>:<account-id>:lgw:<lgw-id>                       |
| vif            | dcaas:<region>:<account-id>:vif:<vif-id>                       |
| lgwTable       | dcaas:<region>:<account-id>:lgwTable:<lgwTable-id>             |
| gdgw           | dcaas:<region>:<account-id>:gdgw:<gdgw-id>                     |
| vifPeer        | dcaas:<region>:<account-id>:vifPeer:<vifPeer-id>               |
| vpc            | vpc:<region>:<account-id>:vpc:<vpc-id>                         |
| vgw            | dcaas:<region>:<account-id>:vgw:<vgw-id>                       |
| directConnect  | dcaas:<region>:<account-id>:directConnect:<directConnect-id>   |
| lag            | dcaas:<region>:<account-id>:lag:<lag-id>                       |
| connectGateway | dcaas:<region>:<account-id>:connectGateway:<connectGateway-id> |

## Conditions

DC does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.3.5 VPC Endpoint

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by VPCEP, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by VPCEP, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for VPCEP.

**Table 3-53** Actions supported by VPCEP

| Action                 | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                          | Alias |
|------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-------|
| vpcep:endpoints:create | Grants permission to create a VPC endpoint for a specified service. | Write        | endpoints *                 | <ul style="list-style-type: none"> <li>vpcep:VpcServiceName</li> <li>vpcep:VpcServiceOrgPath</li> <li>vpcep:VpcServiceOwner</li> </ul> | -     |
|                        |                                                                     |              | vpc *                       | -                                                                                                                                      |       |
|                        |                                                                     |              | route Table                 | -                                                                                                                                      |       |
|                        |                                                                     |              | subnet                      | -                                                                                                                                      |       |
|                        |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> <li>g:EnterpriseProjectId</li> </ul>       |       |
| vpcep:endpoints:delete | Grants permission to delete a VPC endpoint.                         | Write        | endpoints *                 | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>vpcep:VpcServiceName</li> </ul>                          | -     |
| vpcep:endpoints:list   | Grants permission to query VPC endpoints.                           | List         | endpoints *                 | -                                                                                                                                      | -     |
|                        |                                                                     |              | -                           | g:EnterpriseProjectId                                                                                                                  |       |
| vpcep:endpoints:get    | Grants permission to query details of a VPC endpoint.               | Read         | endpoints *                 | g:ResourceTag/<tag-key>                                                                                                                | -     |



| Action                            | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                         | Alias                    |
|-----------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| vpcep:endpoints:update            | Grants permission to update the Whitelist of a VPC endpoint.               | Write        | endpoints *                 | <ul style="list-style-type: none"> <li>• <a href="#">vpcep:VpcServiceName</a></li> <li>• <a href="#">vpcep:VpcServiceOrgPath</a></li> <li>• <a href="#">vpcep:VpcServiceOwner</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                        |
|                                   |                                                                            |              | route Table                 | -                                                                                                                                                                                                                                                     |                          |
|                                   |                                                                            |              | subnet                      | -                                                                                                                                                                                                                                                     |                          |
| vpcep:endpoints:upgrade           | Upgrade endpoint to endpoint_pro.                                          | Write        | endpoints *                 | <ul style="list-style-type: none"> <li>• <a href="#">vpcep:VpcServiceName</a></li> <li>• <a href="#">vpcep:VpcServiceOrgPath</a></li> <li>• <a href="#">vpcep:VpcServiceOwner</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                        |
| vpcep:endpoints:updateRouteTables | Grants permission to modify the routeTable associated with a VPC endpoint. | Write        | endpoints *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                                         | • vpcep:endpoints:update |
|                                   |                                                                            |              | route Table *               | -                                                                                                                                                                                                                                                     |                          |

| Action                        | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                    | Alias                                                                     |
|-------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| vpcep:endpoints:updatePolicy  | Grants permission to modify the policy of a gateway VPC endpoint. | Write        | endpoints *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | <ul style="list-style-type: none"> <li>vpcep:endpoints:update</li> </ul>  |
| vpcep:endpoints:deletePolicy  | Grants permission to delete the policy of a gateway VPC endpoint. | Write        | endpoints *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | <ul style="list-style-type: none"> <li>vpcep:endpoints:delete</li> </ul>  |
| vpcep:endpointServices:create | Grants permission to create a VPC endpoint service.               | Write        | endpointService *           | <a href="#">vpcep:VpcServicePrivateDnsName</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>vpcep:epservices:create</li> </ul> |
|                               |                                                                   |              | vpc *                       | -                                                                                                                                                                                |                                                                           |
|                               |                                                                   |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                           |
| vpcep:endpointServices:list   | Grants permission to query VPC endpoint services.                 | List         | endpointService *           | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>vpcep:epservices:list</li> </ul>   |
|                               |                                                                   |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            |                                                                           |
| vpcep:endpointServices:get    | Grants permission to query details of a VPC endpoint service.     | Read         | endpointService *           | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | <ul style="list-style-type: none"> <li>vpcep:epservices:get</li> </ul>    |

| Action                                   | Description                                                                                | Access Level          | Resource Type (*: required) | Condition Key                                 | Alias                                                                      |
|------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------|
| vpcep:endpointServices:update            | Grants permission to modify a VPC endpoint service.                                        | Write                 | endpointServices *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>vpcep:epservices:update</li> </ul>  |
| vpcep:endpointServices:delete            | Grants permission to delete a VPC endpoint service.                                        | Write                 | endpointServices *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>vpcep:epservices:delete</li> </ul>  |
| vpcep:endpointServices:updateName        | Grants permission to change the name of a VPC endpoint service.                            | Write                 | endpointServices *          | -                                             | <ul style="list-style-type: none"> <li>vpcep:epservices:update</li> </ul>  |
| vpcep:endpointServices:describe          | Grants permission to query description a VPC endpoint service.                             | Read                  | -                           | -                                             | <ul style="list-style-type: none"> <li>vpcep:epserviceDescribe</li> </ul>  |
| vpcep:endpointServices:listPublic        | Grants permission to query public endpoint services.                                       | List                  | endpointServices *          | -                                             | <ul style="list-style-type: none"> <li>vpcep:pubEpservices:list</li> </ul> |
| vpcep:endpointServices:listPermissions   | Grants permission to whitelist records of a VPC endpoint service.                          | List                  | endpointServices *          | -                                             | <ul style="list-style-type: none"> <li>vpcep:permissions:list</li> </ul>   |
| vpcep:endpointServices:updatePermissions | Grants permission to batch adding or deleting whitelist records of a VPC Endpoint Service. | Permission management | endpointServices *          | -                                             | <ul style="list-style-type: none"> <li>vpcep:permissions:update</li> </ul> |

| Action                                              | Description                                                                                    | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                      |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
|                                                     |                                                                                                |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">vpcep:VpcEndpointOrgPath</a></li> <li>• <a href="#">vpcep:VpcEndpointOwner</a></li> </ul> |                            |
| vpcep:endpointServices:createPermissions            | Grants permission to batch adding whitelist records of a VPC Endpoint Service.                 | Permission_management | endpointServices *          | -                                                                                                                                              | • vpcep:permissions:update |
|                                                     |                                                                                                |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">vpcep:VpcEndpointOrgPath</a></li> <li>• <a href="#">vpcep:VpcEndpointOwner</a></li> </ul> |                            |
| vpcep:endpointServices:deletePermissions            | Grants permission to batch deleting whitelist records of a VPC Endpoint Service.               | Permission_management | endpointServices *          | -                                                                                                                                              | • vpcep:permissions:update |
| vpcep:endpointServices:updatePermissionsDescription | Grants permission to updating the description of a whitelist record of a VPC endpoint service. | Write                 | endpointServices *          | -                                                                                                                                              | • vpcep:permissions:update |
| vpcep:endpointServices:listConnections              | Grants permission to query connections of a VPC endpoint service.                              | List                  | endpointServices *          | -                                                                                                                                              | • vpcep:connections:list   |

| Action                                             | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                      |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------|
| vpcep:endpointServices:updateConnections           | Grants permission to accept or reject a VPC Endpoint.                                                 | Write        | endpointServices *          | -             | <ul style="list-style-type: none"> <li>vpcep:connections:update</li> </ul> |
| vpcep:endpointServices:updateConnectionDescription | Grants permission to update the description of the VPC endpoint connection.                           | Write        | endpointServices *          | -             | <ul style="list-style-type: none"> <li>vpcep:connections:update</li> </ul> |
| vpcep::listResourceTags                            | Grants permission to query resources by tag.                                                          | List         | endpoints                   | -             | <ul style="list-style-type: none"> <li>vpcep:resource:list</li> </ul>      |
|                                                    |                                                                                                       |              | endpointServices            | -             |                                                                            |
| vpcep::updateResourceTags                          | Grants permission to add or delete resource tags in batches.                                          | Tagging      | endpoints                   | -             | <ul style="list-style-type: none"> <li>vpcep:tags:update</li> </ul>        |
|                                                    |                                                                                                       |              | endpointServices            | -             |                                                                            |
| vpcep::getProjectTags                              | Grants permission to query tags of tenant's resources.                                                | Read         | endpoints                   | -             | <ul style="list-style-type: none"> <li>vpcep:tags:list</li> </ul>          |
|                                                    |                                                                                                       |              | endpointServices            | -             |                                                                            |
| vpcep::listQuotas                                  | Grants permission to query the quota of resources, including VPC endpoint services and VPC endpoints. | Read         | -                           | -             | <ul style="list-style-type: none"> <li>vpcep:quotas:get</li> </ul>         |

| Action                      | Description                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| vpcep::listVersionDetails   | Grants permission to query versions of VPCEP APIs.               | List         | -                           | -             | -     |
| vpcep::listSpecifiedVersion | Grants permission to query the version of a specified VPCEP API. | List         | -                           | -             | -     |

Each API of VPCEP usually supports one or more actions. [Table 3-54](#) lists the supported actions and dependencies.

**Table 3-54** Actions and dependencies supported by VPCEP APIs

| API                                                     | Action                 | Dependencies |
|---------------------------------------------------------|------------------------|--------------|
| POST /v1/{project_id}/vpc-endpoints                     | vpcep:endpoints:create | -            |
| DELETE /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id} | vpcep:endpoints:delete | -            |
| GET /v1/{project_id}/vpc-endpoints                      | vpcep:endpoints:list   | -            |
| GET /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}    | vpcep:endpoints:get    | -            |
| PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}    | vpcep:endpoints:update | -            |

| API                                                                       | Action                            | Dependencies |
|---------------------------------------------------------------------------|-----------------------------------|--------------|
| PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/routetables          | vpcep:endpoints:updateRouteTables | -            |
| PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/policy               | vpcep:endpoints:updatePolicy      | -            |
| DELETE /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}/policy            | vpcep:endpoints:deletePolicy      | -            |
| POST /v1/{project_id}/vpc-endpoint-services                               | vpcep:endpointServices:create     | -            |
| GET /v1/{project_id}/vpc-endpoint-services                                | vpcep:endpointServices:list       | -            |
| GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}      | vpcep:endpointServices:get        | -            |
| PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}      | vpcep:endpointServices:update     | -            |
| DELETE /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}   | vpcep:endpointServices:delete     | -            |
| PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/name | vpcep:endpointServices:updateName | -            |

| API                                                                                              | Action                                              | Dependencies |
|--------------------------------------------------------------------------------------------------|-----------------------------------------------------|--------------|
| GET /v1/{project_id}/vpc-endpoint-services/describe                                              | vpcep:endpointServices:describe                     | -            |
| GET /v1/{project_id}/vpc-endpoint-services/public                                                | vpcep:endpointServices:listPublic                   | -            |
| GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions                 | vpcep:endpointServices:listPermissions              | -            |
| POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/action         | vpcep:endpointServices:updatePermissions            | -            |
| POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/batch-create   | vpcep:endpointServices:createPermissions            | -            |
| POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/batch-delete   | vpcep:endpointServices:deletePermissions            | -            |
| PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/permissions/{permission_id} | vpcep:endpointServices:updatePermissionsDescription | -            |
| GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections                 | vpcep:endpointServices:listConnections              | -            |



| API                                                                                           | Action                                             | Dependencies |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------|--------------|
| POST /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections/action      | vpcep:endpointServices:updateConnections           | -            |
| PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections/description  | vpcep:endpointServices:updateConnectionDescription | -            |
| POST /v1/{project_id}/{resource_type}/resource_instances/action                               | vpcep::listResourceTags                            | -            |
| POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action                               | vpcep::updateResourceTags                          | -            |
| GET /v1/{project_id}/{resource_type}/tags                                                     | vpcep::getProjectTags                              | -            |
| GET /v1/{project_id}/quotas                                                                   | vpcep::listQuotas                                  | -            |
| GET /                                                                                         | vpcep::listVersionDetails                          | -            |
| GET /{version}                                                                                | vpcep::listSpecifiedVersion                        | -            |
| POST /v2/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/add-server-resources    | vpcep:endpointServices:update                      | -            |
| POST /v2/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/remove-server-resources | vpcep:endpointServices:update                      | -            |

| API                                                                             | Action                                   | Dependencies |
|---------------------------------------------------------------------------------|------------------------------------------|--------------|
| POST /v2/{project_id}/vpc-endpoints/{vpc_endpoint_id}/add-availability-zones    | vpcep:endpointServices:updateConnections | -            |
| POST /v2/{project_id}/vpc-endpoints/{vpc_endpoint_id}/remove-availability-zones | vpcep:endpointServices:updateConnections | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-55](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for VPCEP.

**Table 3-55** Resource types supported by VPCEP

| Resource Type    | URN                                                                |
|------------------|--------------------------------------------------------------------|
| routeTable       | vpc:<region>:<account-id>:routeTable:<route-table-id>              |
| vpc              | vpc:<region>:<account-id>:vpc:<vpc-id>                             |
| endpointServices | vpcep:<region>:<account-id>:endpointServices:<endpoint-service-id> |
| subnet           | vpc:<region>:<account-id>:subnet:<subnet-id>                       |
| endpoints        | vpcep:<region>:<account-id>:endpoints:<endpoint-id>                |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.

- Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, vpcep) apply only to operations of the xx service. For details, see [Table 3-56](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

#### Service-specific condition keys supported by VPCEP

The following table lists the condition keys that you can define in identity policies for VPCEP. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-56** Service-specific condition keys supported by VPCEP

| Service-specific Condition Key  | Type   | Single-valued/<br>Multivalued | Description                                                                                 |
|---------------------------------|--------|-------------------------------|---------------------------------------------------------------------------------------------|
| vpcep:VpceServiceName           | string | Single-valued                 | Filters access by the name of the VPC endpoint service.                                     |
| vpcep:VpceServiceOwner          | string | Single-valued                 | Filters access by the service owner of the VPC endpoint service (huawei, or an account ID). |
| vpcep:VpceServicePrivateDnsName | string | Single-valued                 | Filters access by the vpceServicePrivateDnsName that is passed in the request.              |
| vpcep:VpceServiceOrgPath        | string | Single-valued                 | Filters access by the organization path of the VPC endpoint service owner.                  |

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                        |
|--------------------------------|--------|-------------------------------|--------------------------------------------------------------------|
| vpcep:VpceEndpointOrgPath      | string | Multivalued                   | Filters access by the organization path of the VPC endpoint owner. |
| vpcep:VpceEndpointOwner        | string | Multivalued                   | Filters access by the accountId of VPC endpoint owner.             |

### 3.3.6 Global accelerator

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.

- If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by GA, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by GA, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for GA.

**Table 3-57** Actions supported by GA

| Action                | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| ga:accelerator:list   | Grants permission to list accelerators.     | List         | accelerator *               | -                                                                                                                                                  | -     |
| ga:accelerator:create | Grants permission to create an accelerator. | Write        | accelerator *               | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -     |
|                       |                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| ga:accelerator:get    | Grants permission to get an accelerator.    | Read         | accelerator *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

| Action                | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| ga:accelerator:update | Grants permission to update an accelerator. | Write        | accelerator *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| ga:accelerator:delete | Grants permission to delete an accelerator. | Write        | accelerator *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| ga:listener:list      | Grants permission to list listeners.        | List         | listener *                  | -                                                                                                                                                  | -     |
| ga:listener:create    | Grants permission to create a listener.     | Write        | listener *                  | -                                                                                                                                                  | -     |
|                       |                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| ga:listener:get       | Grants permission to get a listener.        | Read         | listener *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | -     |
| ga:listener:update    | Grants permission to update a listener.     | Write        | listener *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | -     |
| ga:listener:delete    | Grants permission to delete a listener.     | Write        | listener *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | -     |
| ga:endpointgroup:list | Grants permission to list endpoint groups.  | List         | endpointgroup *             | -                                                                                                                                                  | -     |

| Action                  | Description                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                     | Alias |
|-------------------------|------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| ga:endpointgroup:create | Grants permission to create an endpoint group. | Write        | endpointgroup *             | -                                                                                                                                                                 |       |
|                         |                                                |              | -                           | ga:RequestId                                                                                                                                                      |       |
| ga:endpointgroup:get    | Grants permission to get an endpoint group.    | Read         | endpointgroup *             | ga:RegionId                                                                                                                                                       | -     |
| ga:endpointgroup:update | Grants permission to update an endpoint group. | Write        | endpointgroup *             | ga:RegionId                                                                                                                                                       | -     |
| ga:endpointgroup:delete | Grants permission to delete an endpoint group. | Write        | endpointgroup *             | ga:RegionId                                                                                                                                                       | -     |
| ga:endpoint:list        | Grants permission to list endpoints.           | List         | endpoint *                  | -                                                                                                                                                                 | -     |
| ga:endpoint:create      | Grants permission to create an endpoint.       | Write        | endpoint *                  | -                                                                                                                                                                 |       |
|                         |                                                |              | -                           | <ul style="list-style-type: none"> <li>ga:RequestResourceType</li> <li>ga:RequestResourceId</li> <li>ga:RequestIpAddress</li> <li>ga:RequestDomainName</li> </ul> |       |

| Action                | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|-----------------------|--------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| ga:endpoint:get       | Grants permission to get an endpoint.      | Read         | endpoint *                  | <ul style="list-style-type: none"> <li>ga:ResourceType</li> <li>ga:ResourceId</li> <li>ga:IpAddress</li> <li>ga:DomainName</li> </ul> | -     |
| ga:endpoint:update    | Grants permission to update an endpoint.   | Write        | endpoint *                  | <ul style="list-style-type: none"> <li>ga:ResourceType</li> <li>ga:ResourceId</li> <li>ga:IpAddress</li> <li>ga:DomainName</li> </ul> | -     |
| ga:endpoint:delete    | Grants permission to delete an endpoint.   | Write        | endpoint *                  | <ul style="list-style-type: none"> <li>ga:ResourceType</li> <li>ga:ResourceId</li> <li>ga:IpAddress</li> <li>ga:DomainName</li> </ul> | -     |
| ga:healthcheck:list   | Grants permission to list health checks.   | List         | healthcheck *               | -                                                                                                                                     | -     |
| ga:healthcheck:create | Grants permission to create a healthcheck. | Write        | healthcheck *               | -                                                                                                                                     | -     |
| ga:healthcheck:get    | Grants permission to get a healthcheck.    | Read         | healthcheck *               | -                                                                                                                                     | -     |



| Action                 | Description                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias                     |
|------------------------|-----------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| ga:healthcheck:update  | Grants permission to update a healthcheck.                | Write        | healthcheck *               | -                                                                                                                                 | -                         |
| ga:healthcheck:delete  | Grants permission to delete a healthcheck.                | Write        | healthcheck *               | -                                                                                                                                 | -                         |
| ga:tag:create          | Grants permission to create tags for a resource.          | Tagging      | accelerator                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                         |
|                        |                                                           |              | listener                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                           |
|                        |                                                           |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                           |
| ga:tag:delete          | Grants permission to delete tags of a specified resource. | Tagging      | accelerator *               | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                         |
|                        |                                                           |              | listener *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                           |
|                        |                                                           |              | -                           | <a href="#">g:TagKeys</a>                                                                                                         |                           |
| ga:tag:get             | Grants permission to query tags of resource.              | Read         | accelerator                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                         |
|                        |                                                           |              | listener                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                           |
| ga:tag:list            | Grants permission to list tags.                           | List         | -                           | -                                                                                                                                 | -                         |
| ga::listResourcesByTag | Grants permission to list resource instances by tag.      | List         | -                           | <a href="#">g:TagKeys</a>                                                                                                         | ga:tag:listResourcesByTag |
| ga:ipgroup:list        | Grants permission to list ip groups.                      | List         | ipgroup *                   | -                                                                                                                                 | -                         |

| Action                          | Description                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ga:ipgroup:create               | Grants permission to create an ip group.                            | Write        | ipgroup *                   | -             | -     |
| ga:ipgroup:get                  | Grants permission to get an ip group.                               | Read         | ipgroup *                   | -             | -     |
| ga:ipgroup:update               | Grants permission to update an ip group.                            | Write        | ipgroup *                   | -             | -     |
| ga:ipgroup:delete               | Grants permission to delete an ip group.                            | Write        | ipgroup *                   | -             | -     |
| ga:ipgroup:addips               | Grants permission to add ips of a specified ip group.               | Write        | ipgroup *                   | -             | -     |
| ga:ipgroup:removelps            | Grants permission to remove ips of a specified ip group.            | Write        | ipgroup *                   | -             | -     |
| ga:ipgroup:associateListener    | Grants permission to associate listener of a specified ip group.    | Write        | ipgroup *                   | -             | -     |
| ga:ipgroup:disassociateListener | Grants permission to disassociate listener of a specified ip group. | Write        | ipgroup *                   | -             | -     |

| Action             | Description                            | Access Level | Resource Type (*: required) | Condition Key | Alias             |
|--------------------|----------------------------------------|--------------|-----------------------------|---------------|-------------------|
| ga::listByoipPools | Grants permission to list byoip pools. | List         | -                           | -             | ga:byoippool:list |
| ga:logtank:list    | Grants permission to list logtanks.    | List         | logtank *                   | -             | -                 |
| ga:logtank:create  | Grants permission to create logtank.   | Write        | logtank *                   | -             | -                 |
| ga:logtank:get     | Grants permission to get logtank info. | Read         | logtank *                   | -             | -                 |
| ga:logtank:update  | Grants permission to modify logtank.   | Write        | logtank *                   | -             | -                 |
| ga:logtank:delete  | Grants permission to delete logtank.   | Write        | logtank *                   | -             | -                 |

Each API of GA usually supports one or more actions. [Table 3-58](#) lists the supported actions and dependencies.

**Table 3-58** Actions and dependencies supported by GA APIs

| API                                   | Action                | Dependencies |
|---------------------------------------|-----------------------|--------------|
| GET /v1/accelerators                  | ga:accelerator:list   | -            |
| POST /v1/accelerators                 | ga:accelerator:create | -            |
| GET /v1/accelerators/{accelerator_id} | ga:accelerator:get    | -            |

| API                                                                 | Action                  | Dependencies |
|---------------------------------------------------------------------|-------------------------|--------------|
| PUT /v1/accelerators/{accelerator_id}                               | ga:accelerator:update   | -            |
| DELETE /v1/accelerators/{accelerator_id}                            | ga:accelerator:delete   | -            |
| GET /v1/listeners                                                   | ga:listener:list        | -            |
| POST /v1/listeners                                                  | ga:listener:create      | -            |
| GET /v1/listeners/{listener_id}                                     | ga:listener:get         | -            |
| PUT /v1/listeners/{listener_id}                                     | ga:listener:update      | -            |
| DELETE /v1/listeners/{listener_id}                                  | ga:listener:delete      | -            |
| GET /v1/endpoint-groups                                             | ga:endpointgroup:list   | -            |
| POST /v1/endpoint-groups                                            | ga:endpointgroup:create | -            |
| GET /v1/endpoint-groups/{endpoint_group_id}                         | ga:endpointgroup:get    | -            |
| PUT /v1/endpoint-groups/{endpoint_group_id}                         | ga:endpointgroup:update | -            |
| DELETE /v1/endpoint-groups/{endpoint_group_id}                      | ga:endpointgroup:delete | -            |
| GET /v1/endpoint-groups/{endpoint_group_id}/endpoints               | ga:endpoint:list        | -            |
| POST /v1/endpoint-groups/{endpoint_group_id}/endpoints              | ga:endpoint:create      | -            |
| GET /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id} | ga:endpoint:get         | -            |

| API                                                                    | Action                 | Dependencies |
|------------------------------------------------------------------------|------------------------|--------------|
| PUT /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id}    | ga:endpoint:update     | -            |
| DELETE /v1/endpoint-groups/{endpoint_group_id}/endpoints/{endpoint_id} | ga:endpoint:delete     | -            |
| GET /v1/health-checks                                                  | ga:healthcheck:list    | -            |
| POST /v1/health-checks                                                 | ga:healthcheck:create  | -            |
| GET /v1/health-checks/{health_check_id}                                | ga:healthcheck:get     | -            |
| PUT /v1/health-checks/{health_check_id}                                | ga:healthcheck:update  | -            |
| DELETE /v1/health-checks/{health_check_id}                             | ga:healthcheck:delete  | -            |
| POST /v1/{resource_type}/{resource_id}/tags/create                     | ga:tag:create          | -            |
| DELETE /v1/{resource_type}/{resource_id}/tags/delete                   | ga:tag:delete          | -            |
| GET /v1/{resource_type}/{resource_id}/tags                             | ga:tag:get             | -            |
| POST /v1/{resource_type}/resource-instances/filter                     | ga::listResourcesByTag | -            |
| POST /v1/{resource_type}/resource-instances/count                      | ga::listResourcesByTag | -            |

| API                                                    | Action                          | Dependencies |
|--------------------------------------------------------|---------------------------------|--------------|
| GET /v1/{resource_type}/tags                           | ga:tag:list                     | -            |
| GET /v1/ip-groups                                      | ga:ipgroup:list                 | -            |
| POST /v1/ip-groups                                     | ga:ipgroup:create               | -            |
| GET /v1/ip-groups/{ip_group_id}                        | ga:ipgroup:get                  | -            |
| PUT /v1/ip-groups/{ip_group_id}                        | ga:ipgroup:update               | -            |
| DELETE /v1/ip-groups/{ip_group_id}                     | ga:ipgroup:delete               | -            |
| POST /v1/ip-groups/{ip_group_id}/add-ips               | ga:ipgroup:addIps               | -            |
| POST /v1/ip-groups/{ip_group_id}/remove-ips            | ga:ipgroup:removeIps            | -            |
| POST /v1/ip-groups/{ip_group_id}/associate-listener    | ga:ipgroup:associateListener    | -            |
| POST /v1/ip-groups/{ip_group_id}/disassociate-listener | ga:ipgroup:disassociateListener | -            |
| GET /v1/byoip-pools                                    | ga::listByoipPools              | -            |
| GET /v1/logtanks                                       | ga:logtank:list                 | -            |
| POST /v1/logtanks                                      | ga:logtank:create               | -            |
| GET /v1/logtanks/{logtank_id}                          | ga:logtank:get                  | -            |
| PUT /v1/logtanks/{logtank_id}                          | ga:logtank:update               | -            |
| DELETE /v1/logtanks/{logtank_id}                       | ga:logtank:delete               | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-59](#), the resource URN must be

specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for GA.

**Table 3-59** Resource types supported by GA

| Resource Type | URN                                               |
|---------------|---------------------------------------------------|
| ipgroup       | ga::<account-id>:ipgroup:<ipgroup-id>             |
| endpoint      | ga::<account-id>:endpoint:<endpoint-id>           |
| accelerator   | ga::<account-id>:accelerator:<accelerator-id>     |
| logtank       | ga::<account-id>:logtank:<logtank-id>             |
| listener      | ga::<account-id>:listener:<listener-id>           |
| healthcheck   | ga::<account-id>:healthcheck:<healthcheck-id>     |
| endpointgroup | ga::<account-id>:endpointgroup:<endpointgroup-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, ga) apply only to operations of the xx service. For details, see [Table 3-60](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when

its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by GA

The following table lists the condition keys that you can define in identity policies for GA. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-60** Service-specific condition keys supported by GA

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                        |
|--------------------------------|--------|-------------------------------|--------------------------------------------------------------------|
| ga:RequestRegionId             | string | Single-valued                 | Filters access by the region id that is passed in the request.     |
| ga:RequestResource-Type        | string | Single-valued                 | Filters access by the resource type that is passed in the request. |
| ga:RequestResourceId           | string | Single-valued                 | Filters access by the resource id that is passed in the request.   |
| ga:RequestIpAddress            | string | Single-valued                 | Filters access by the ip address that is passed in the request.    |
| ga:RequestDomainName           | string | Single-valued                 | Filters access by the domain name that is passed in the request.   |
| ga:RegionId                    | string | Single-valued                 | Filters access by endpoint-group region id.                        |
| ga:ResourceType                | string | Single-valued                 | Filters access by endpoint resource type.                          |
| ga:ResourceId                  | string | Single-valued                 | Filters access by endpoint resource id.                            |
| ga:IpAddress                   | string | Single-valued                 | Filters access by endpoint ip address.                             |
| ga:DomainName                  | string | Single-valued                 | Filters access by endpoint domain name.                            |



### 3.3.7 NAT Gateway

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by NAT, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by NAT, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for NAT.

**Table 3-61** Actions supported by NAT

| Action                        | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|-------------------------------|--------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| nat:privateNatGateways:list   | Grants permission to query private NAT gateways.             | List         | privateGateway *            | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| nat:privateNatGateways:create | Grants permission to create a private NAT gateway.           | Write        | privateGateway *            | -                                                                                                                                                                                      | -     |
|                               |                                                              |              | subnet *                    | -                                                                                                                                                                                      |       |
|                               |                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| nat:privateNatGateways:delete | Grants permission to delete a specified private NAT gateway. | Write        | privateGateway *            | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| nat:privateNatGateways:get    | Grants permission to query a specified private NAT gateway.  | Read         | privateGateway *            | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |

| Action                         | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|--------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| nat:privateNatGateways:update  | Grants permission to update a specified private NAT gateway.                | Write        | privateGateway *            | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| nat:privateNatDnatRules:list   | Grants permission to query DNAT rules of private NAT gateways.              | List         | privateDnatRule *           | g:EnterpriseProjectId                                                                                          | -     |
| nat:privateNatDnatRules:create | Grants permission to create a DNAT rule for a private NAT gateway.          | Write        | privateGateway *            | g:ResourceTag/<tag-key>                                                                                        | -     |
|                                |                                                                             |              | privateDnatRule *           | -                                                                                                              |       |
|                                |                                                                             |              | privateTransitIp *          | g:ResourceTag/<tag-key>                                                                                        |       |
|                                |                                                                             |              | port                        | -                                                                                                              |       |
|                                |                                                                             |              | -                           | g:EnterpriseProjectId                                                                                          |       |
| nat:privateNatDnatRules:delete | Grants permission to delete a specified DNAT rule of a private NAT gateway. | Write        | privateGateway *            | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                                |                                                                             |              | privateDnatRule *           | g:EnterpriseProjectId                                                                                          |       |

| Action                         | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| nat:privateNatDnatRules:get    | Grants permission to query a specified DNAT rule of a private NAT gateway.  | Read         | privateGateway *            | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                |                                                                             |              | privateDnatRule *           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| nat:privateNatDnatRules:update | Grants permission to update a specified DNAT rule of a private NAT gateway. | Write        | privateGateway *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | -     |
|                                |                                                                             |              | privateDnatRule *           | -                                                                                                                                                  |       |
|                                |                                                                             |              | privateTransitIp            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      |       |
|                                |                                                                             |              | port                        | -                                                                                                                                                  |       |
|                                |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| nat:privateNatSnatRules:list   | Grants permission to query SNAT rules of private NAT gateways.              | List         | privateSnatRule *           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -     |
| nat:privateNatSnatRules:create | Grants permission to create an SNAT rule for a private NAT gateway.         | Write        | privateGateway *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | -     |
|                                |                                                                             |              | privateSnatRule *           | -                                                                                                                                                  |       |
|                                |                                                                             |              | privateTransitIp *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      |       |

| Action                         | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias               |
|--------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                |                                                                             |              | subnet                      | -                                                                                                                                              |                     |
|                                |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                     |
| nat:privateNatSnatRules:delete | Grants permission to delete a specified SNAT rule of a private NAT gateway. | Write        | privateGateway *            | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                   |
|                                |                                                                             |              | privateSnatRule *           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                     |
| nat:privateNatSnatRules:get    | Grants permission to query a specified SNAT rule of a private NAT gateway.  | Read         | privateGateway *            | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                   |
|                                |                                                                             |              | privateSnatRule *           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                     |
| nat:privateNatSnatRules:update | Grants permission to update a specified SNAT rule of a private NAT gateway. | Write        | privateGateway *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -                   |
|                                |                                                                             |              | privateSnatRule *           | -                                                                                                                                              |                     |
|                                |                                                                             |              | privateTransitIp            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  |                     |
|                                |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                     |
| nat:privateNatTransitIps:list  | Grants permission to query private NAT transit IP addresses.                | List         | privateTransitIp *          | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | nat:transitIps:list |

| Action                          | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                    | Alias                  |
|---------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| nat:privateNatTransitIps:create | Grants permission to create a private NAT transit IP address.           | Write        | privateTransitIp *          | -                                                                                                                                                                                | nat:transitIps: create |
|                                 |                                                                         |              | subnet                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    |                        |
|                                 |                                                                         |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                        |
| nat:privateNatTransitIps:delete | Grants permission to delete a specified private NAT transit IP address. | Write        | privateTransitIp *          | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                   | nat:transitIps: delete |
| nat:privateNatTransitIps:get    | Grants permission to query a specified private NAT transit IP address.  | Read         | privateTransitIp *          | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                   | nat:transitIps: get    |
| nat:transitSubnets:list         | Grants permission to query transit subnets.                             | List         | transitSubnet *             | -                                                                                                                                                                                | -                      |
| nat:transitSubnets:create       | Grants permission to create a transit subnet.                           | Write        | transitSubnet *             | -                                                                                                                                                                                | -                      |
|                                 |                                                                         |              | subnet *                    | -                                                                                                                                                                                |                        |
|                                 |                                                                         |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>                                                |                        |

| Action                            | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                            |
|-----------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| nat:transitSubnets:delete         | Grants permission to delete a specified transit subnet.               | Write        | transitSubnet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -                                |
| nat:transitSubnets:get            | Grants permission to query a specified transit subnet.                | Read         | transitSubnet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -                                |
| nat:transitSubnets:update         | Grants permission to update a specified transit subnet.               | Write        | transitSubnet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -                                |
| nat:privateNatGateways:createTags | Grants permission to create tags for a specified private NAT gateway. | Tagging      | privateGateway *            | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | nat:privateNatGatewayTags:create |
|                                   |                                                                       |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              |                                  |
| nat:privateNatGateways:deleteTags | Grants permission to delete tags of a specified private NAT gateway.  | Tagging      | privateGateway *            | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | nat:privateNatGatewayTags:delete |
|                                   |                                                                       |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              |                                  |

| Action                              | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                          |
|-------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| nat:privateNatGateways:listTags     | Grants permission to query tags of private NAT gateways.                         | List         | privateGateway              | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | nat:privateNatGatewayTags:list |
| nat:privateNatTransitIps:createTags | Grants permission to create tags for a specified private NAT transit IP address. | Tagging      | privateTransitIp *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | nat:transitIpTags:create       |
|                                     |                                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                |
| nat:privateNatTransitIps:deleteTags | Grants permission to delete tags of a specified private NAT transit IP address.  | Tagging      | privateTransitIp *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | nat:transitIpTags:delete       |
|                                     |                                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                                |
| nat:privateNatTransitIps:listTags   | Grants permission to query tags of private NAT transit IP addresses.             | List         | privateTransitIp            | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | nat:transitIpTags:list         |
| nat:transitSubnets:createTags       | Grants permission to create tags for a specified transit subnet.                 | Tagging      | transitSubnet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | nat:transitSubnetTags:create   |



| Action                        | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                    | Alias                        |
|-------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
|                               |                                                                 |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>                                                |                              |
| nat:transitSubnets:deleteTags | Grants permission to delete tags of a specified transit subnet. | Tagging      | transitSubnet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | nat:transitSubnetTags:delete |
|                               |                                                                 |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>                                                |                              |
| nat:transitSubnets:listTags   | Grants permission to query tags of transit subnets.             | List         | transitSubnet               | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | nat:transitSubnetTags:list   |
| nat:natGateways:list          | Grants permission to query public NAT gateways.                 | List         | gateway *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                            | -                            |
| nat:natGateways:create        | Grants permission to create a public NAT gateway.               | Write        | gateway *                   | -                                                                                                                                                                                | -                            |
|                               |                                                                 |              | vpc *                       | -                                                                                                                                                                                |                              |
|                               |                                                                 |              | subnet *                    | -                                                                                                                                                                                |                              |
|                               |                                                                 |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                              |

| Action                 | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| nat:natGateways:delete | Grants permission to delete a specified public NAT gateway.       | Write        | gateway *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| nat:natGateways:get    | Grants permission to query a specified public NAT gateway.        | Read         | gateway *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| nat:natGateways:update | Grants permission to update a specified public NAT gateway.       | Write        | gateway *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| nat:dnatRules:list     | Grants permission to query DNAT rules of public NAT gateways.     | List         | dnatRule *                  | g:EnterpriseProjectId                                                                                          | -     |
| nat:dnatRules:create   | Grants permission to create a DNAT rule for a public NAT gateway. | Write        | gateway *                   | g:ResourceTag/<tag-key>                                                                                        | -     |
|                        |                                                                   |              | dnatRule *                  | -                                                                                                              |       |
|                        |                                                                   |              | publicip                    | -                                                                                                              |       |
|                        |                                                                   |              | globalEip                   | -                                                                                                              |       |
|                        |                                                                   |              | port                        | -                                                                                                              |       |
|                        |                                                                   |              | -                           | g:EnterpriseProjectId                                                                                          |       |

| Action                | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| nat:dnatRules: get    | Grants permission to query a specified DNAT rule of a public NAT gateway.   | Read         | gateway *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                       |                                                                             |              | dnatRule *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| nat:dnatRules: update | Grants permission to update a specified DNAT rule of a public NAT gateway.  | Write        | gateway *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | -     |
|                       |                                                                             |              | dnatRule *                  | -                                                                                                                                                  |       |
|                       |                                                                             |              | publicip                    | -                                                                                                                                                  |       |
|                       |                                                                             |              | globalEip                   | -                                                                                                                                                  |       |
|                       |                                                                             |              | port                        | -                                                                                                                                                  |       |
|                       |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| nat:dnatRules: delete | Grants permission to delete a specified DNAT rule of a private NAT gateway. | Write        | gateway *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                       |                                                                             |              | dnatRule *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |       |
| nat:snatRules: list   | Grants permission to query SNAT rules of public NAT gateways.               | List         | snatRule *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -     |

| Action                | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias |
|-----------------------|----------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| nat:snatRules: create | Grants permission to create a SNAT rule for a public NAT gateway.          | Write        | gateway *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -     |
|                       |                                                                            |              | snatRule *                  | -                                                                                                                                              |       |
|                       |                                                                            |              | publicip                    | -                                                                                                                                              |       |
|                       |                                                                            |              | globalEip                   | -                                                                                                                                              |       |
|                       |                                                                            |              | subnet                      | -                                                                                                                                              |       |
|                       |                                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |       |
| nat:snatRules: get    | Grants permission to query a specified SNAT rule of a public NAT gateway.  | Read         | gateway *                   | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                       |                                                                            |              | snatRule *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |       |
| nat:snatRules: update | Grants permission to update a specified SNAT rule of a public NAT gateway. | Write        | gateway *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -     |
|                       |                                                                            |              | snatRule *                  | -                                                                                                                                              |       |
|                       |                                                                            |              | publicip                    | -                                                                                                                                              |       |
|                       |                                                                            |              | globalEip                   | -                                                                                                                                              |       |
|                       |                                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |       |
|                       |                                                                            |              |                             |                                                                                                                                                |       |

| Action                     | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                     |
|----------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| nat:snatRules:delete       | Grants permission to delete a specified SNAT rule of a private NAT gateway. | Write        | gateway *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                         |
|                            |                                                                             |              | snatRule *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                           |
| nat:natGateways:createTags | Grants permission to create tags for a specified public NAT gateway.        | Tagging      | gateway *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | nat:natGatewayTags:create |
|                            |                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                           |
| nat:natGateways:deleteTags | Grants permission to delete tags of a specified public NAT gateway.         | Tagging      | gateway *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | nat:natGatewayTags:delete |
|                            |                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                           |
| nat:natGateways:listTags   | Grants permission to query tags of public NAT gateways.                     | List         | gateway                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | nat:natGatewayTags:get    |

Each API of NAT usually supports one or more actions. [Table 3-62](#) lists the supported actions and dependencies.

**Table 3-62** Actions and dependencies supported by NAT APIs

| API                                                           | Action                         | Dependencies |
|---------------------------------------------------------------|--------------------------------|--------------|
| GET /v3/{project_id}/private-nat/gateways                     | nat:privateNatGateways:list    | -            |
| POST /v3/{project_id}/private-nat/gateways                    | nat:privateNatGateways:create  | -            |
| DELETE /v3/{project_id}/private-nat/gateways/{gateway_id}     | nat:privateNatGateways:delete  | -            |
| GET /v3/{project_id}/private-nat/gateways/{gateway_id}        | nat:privateNatGateways:get     | -            |
| PUT /v3/{project_id}/private-nat/gateways/{gateway_id}        | nat:privateNatGateways:update  | -            |
| GET /v3/{project_id}/private-nat/dnat-rules                   | nat:privateNatDnatRules:list   | -            |
| POST /v3/{project_id}/private-nat/dnat-rules                  | nat:privateNatDnatRules:create | -            |
| DELETE /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id} | nat:privateNatDnatRules:delete | -            |
| GET /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}    | nat:privateNatDnatRules:get    | -            |
| PUT /v3/{project_id}/private-nat/dnat-rules/{dnat_rule_id}    | nat:privateNatDnatRules:update | -            |
| GET /v3/{project_id}/private-nat/snat-rules                   | nat:privateNatSnatRules:list   | -            |

| API                                                                  | Action                            | Dependencies                      |
|----------------------------------------------------------------------|-----------------------------------|-----------------------------------|
| POST /v3/{project_id}/private-nat/snat-rules                         | nat:privateNatSnatRules:create    | -                                 |
| DELETE /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}        | nat:privateNatSnatRules:delete    | -                                 |
| GET /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}           | nat:privateNatSnatRules:get       | -                                 |
| PUT /v3/{project_id}/private-nat/snat-rules/{snat_rule_id}           | nat:privateNatSnatRules:update    | -                                 |
| GET /v3/{project_id}/private-nat/transit-ips                         | nat:privateNatTransitIps:list     | -                                 |
| POST /v3/{project_id}/private-nat/transit-ips                        | nat:privateNatTransitIps:create   | -                                 |
| DELETE /v3/{project_id}/private-nat/transit-ips/{transit_ip_id}      | nat:privateNatTransitIps:delete   | -                                 |
| GET /v3/{project_id}/private-nat/transit-ips/{transit_ip_id}         | nat:privateNatTransitIps:get      | -                                 |
| POST /v3/{project_id}/private-nat-gateways/resource_instances/action | nat:privateNatGateways:listTags   | -                                 |
| POST /v3/{project_id}/private-nat-gateways/{resource_id}/tags/action | nat:privateNatGateways:createTags | nat:privateNatGateways:deleteTags |
| POST /v3/{project_id}/private-nat-gateways/{resource_id}/tags        | nat:privateNatGateways:createTags | -                                 |

| API                                                                     | Action                              | Dependencies                        |
|-------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| GET /v3/{project_id}/private-nat-gateways/{resource_id}/tags            | nat:privateNatGateways:listTags     | -                                   |
| DELETE /v3/{project_id}/private-nat-gateways/{resource_id}/tags/{key}   | nat:privateNatGateways:deleteTags   | -                                   |
| GET /v3/{project_id}/private-nat-gateways/tags                          | nat:privateNatGateways:listTags     | -                                   |
| POST /v3/{project_id}/transit-ips/resource_instances/action             | nat:privateNatTransitIps:listTags   | -                                   |
| POST /v3/{project_id}/transit-ips/{resource_id}/tags/action             | nat:privateNatTransitIps:createTags | nat:privateNatTransitIps:deleteTags |
| POST /v3/{project_id}/transit-ips/{resource_id}/tags                    | nat:privateNatTransitIps:createTags | -                                   |
| GET /v3/{project_id}/transit-ips/{resource_id}/tags                     | nat:privateNatTransitIps:listTags   | -                                   |
| DELETE /v3/{project_id}/transit-ips/{resource_id}/tags/{key}            | nat:privateNatTransitIps:deleteTags | -                                   |
| GET /v3/{project_id}/transit-ips/tags                                   | nat:privateNatTransitIps:listTags   | -                                   |
| POST /v3/{project_id}/private-nat/transit-subnets                       | nat:transitSubnets:create           | -                                   |
| DELETE /v3/{project_id}/private-nat/transit-subnets/{transit_subnet_id} | nat:transitSubnets:delete           | -                                   |



| API                                                                  | Action                        | Dependencies                  |
|----------------------------------------------------------------------|-------------------------------|-------------------------------|
| GET /v3/{project_id}/private-nat/transit-subnets/{transit_subnet_id} | nat:transitSubnets:get        | -                             |
| PUT /v3/{project_id}/private-nat/transit-subnets/{transit_subnet_id} | nat:transitSubnets:update     | -                             |
| POST /v3/{project_id}/transit-subnets/resource_instances/action      | nat:transitSubnets:listTags   | -                             |
| POST /v3/{project_id}/transit-subnets/{resource_id}/tags/action      | nat:transitSubnets:createTags | nat:transitSubnets:deleteTags |
| POST /v3/{project_id}/transit-subnets/{resource_id}/tags             | nat:transitSubnets:createTags | -                             |
| GET /v3/{project_id}/transit-subnets/{resource_id}/tags              | nat:transitSubnets:listTags   | -                             |
| DELETE /v3/{project_id}/transit-subnets/{resource_id}/tags/{key}     | nat:transitSubnets:deleteTags | -                             |
| GET /v3/{project_id}/transit-subnets/tags                            | nat:transitSubnets:listTags   | -                             |
| GET /v2/{project_id}/nat_gateways                                    | nat:natGateways:list          | -                             |
| POST /v2/{project_id}/nat_gateways                                   | nat:natGateways:create        | -                             |

| API                                                                             | Action                 | Dependencies                                                                                                                  |
|---------------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}                           | nat:natGateways:delete | -                                                                                                                             |
| GET /v2/{project_id}/nat_gateways/{nat_gateway_id}                              | nat:natGateways:get    | -                                                                                                                             |
| PUT /v2/{project_id}/nat_gateways/{nat_gateway_id}                              | nat:natGateways:update | -                                                                                                                             |
| GET /v2/{project_id}/dnat_rules                                                 | nat:dnatRules:list     | -                                                                                                                             |
| POST /v2/{project_id}/dnat_rules                                                | nat:dnatRules:create   | eip:publicIps:associateInstance                                                                                               |
| GET /v2/{project_id}/dnat_rules/{dnat_rule_id}                                  | nat:dnatRules:get      | -                                                                                                                             |
| PUT /v2/{project_id}/dnat_rules/{dnat_rule_id}                                  | nat:dnatRules:update   | <ul style="list-style-type: none"> <li>eip:publicIps:associateInstance</li> <li>eip:publicIps:disassociateInstance</li> </ul> |
| POST /v2/{project_id}/dnat_rules/batch                                          | nat:dnatRules:create   | eip:publicIps:associateInstance                                                                                               |
| DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}/dnat_rules/{dnat_rule_id} | nat:dnatRules:delete   | eip:publicIps:disassociateInstance                                                                                            |
| GET /v2/{project_id}/snat_rules                                                 | nat:snatRules:list     | -                                                                                                                             |
| POST /v2/{project_id}/snat_rules                                                | nat:snatRules:create   | eip:publicIps:associateInstance                                                                                               |

| API                                                                                                 | Action                     | Dependencies                                                                                                                  |
|-----------------------------------------------------------------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| GET /v2/<br>{project_id}/<br>snat_rules/<br>{snat_rule_id}                                          | nat:snatRules:get          | -                                                                                                                             |
| PUT /v2/<br>{project_id}/<br>snat_rules/<br>{snat_rule_id}                                          | nat:snatRules:update       | <ul style="list-style-type: none"> <li>eip:publicIps:associateInstance</li> <li>eip:publicIps:disassociateInstance</li> </ul> |
| DELETE /v2/<br>{project_id}/<br>nat_gateways/<br>{nat_gateway_id}/<br>snat_rules/<br>{snat_rule_id} | nat:snatRules:delete       | eip:publicIps:disassociateInstance                                                                                            |
| POST /v3/<br>{project_id}/<br>nat_gateways/<br>resource_instances/<br>action                        | nat:natGateways:listTags   | -                                                                                                                             |
| POST /v3/<br>{project_id}/<br>nat_gateways/<br>{nat_gateway_id}/<br>tags/action                     | nat:natGateways:createTags | nat:natGateways:deleteTags                                                                                                    |
| POST /v3/<br>{project_id}/<br>nat_gateways/<br>{nat_gateway_id}/<br>tags                            | nat:natGateways:createTags | -                                                                                                                             |
| GET /v3/<br>{project_id}/<br>nat_gateways/<br>{nat_gateway_id}/<br>tags                             | nat:natGateways:listTags   | -                                                                                                                             |
| DELETE /v3/<br>{project_id}/<br>nat_gateways/<br>{nat_gateway_id}/<br>tags/{key}                    | nat:natGateways:deleteTags | -                                                                                                                             |
| GET /v3/<br>{project_id}/<br>nat_gateways/tags                                                      | nat:natGateways:listTags   | -                                                                                                                             |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-63](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for NAT.

**Table 3-63** Resource types supported by NAT

| Resource Type    | URN                                                                |
|------------------|--------------------------------------------------------------------|
| snatRule         | nat:<region>:<account-id>:snatRule:<snat-rule-id>                  |
| privateSnatRule  | nat:<region>:<account-id>:privateSnatRule:<private-snat-rule-id>   |
| port             | vpc:<region>:<account-id>:port:<port-id>                           |
| privateGateway   | nat:<region>:<account-id>:privateGateway:<private-gateway-id>      |
| vpc              | vpc:<region>:<account-id>:vpc:<vpc-id>                             |
| publicip         | vpc:<region>:<account-id>:publicip:<publicip-id>                   |
| gateway          | nat:<region>:<account-id>:gateway:<gateway-id>                     |
| privateTransitIp | nat:<region>:<account-id>:privateTransitIp:<private-transit-ip-id> |
| dnatRule         | nat:<region>:<account-id>:dnatRule:<dnat-rule-id>                  |
| globalEip        | eip:<region>:<account-id>:globalEip:<geip-id>                      |
| privateDnatRule  | nat:<region>:<account-id>:privateDnatRule:<private-dnat-rule-id>   |
| subnet           | vpc:<region>:<account-id>:subnet:<subnet-id>                       |
| transitSubnet    | nat:<region>:<account-id>:transitSubnet:<transit-subnet-id>        |

## Conditions

NAT does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.3.8 Cloud Connect

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CC, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CC, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CC.

**Table 3-64** Actions supported by CC

| Action                     | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|----------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cc:cloudConnections:create | Grants permission to create a cloud connection.               | Write        | cloud Connection *          | -                                                                                                                                                                                      | -     |
|                            |                                                               |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| cc:cloudConnections:delete | Grants permission to delete a cloud connection.               | Write        | cloud Connection *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| cc:cloudConnections:update | Grants permission to update a cloud connection.               | Write        | cloud Connection *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| cc:cloudConnections:get    | Grants permission to query the details of a cloud connection. | Read         | cloud Connection *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |

| Action                       | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cc:cloudConnections:list     | Grants permission to query the cloud connections.                | List         | cloud Connection *          | -                                                                                                                                                  | -     |
| cc:cloudConnections:tag      | Grants permission to add tags to a cloud connection.             | Tagging      | cloud Connection *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                              |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| cc:cloudConnections:unTag    | Grants permission to delete tags from a cloud connection.        | Tagging      | cloud Connection *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                              |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| cc:cloudConnections:listTags | Grants permission to query the tags added to a cloud connection. | List         | cloud Connection *          | -                                                                                                                                                  | -     |
| cc:networkInstances:create   | Grants permission to create a network instance.                  | Write        | networkInstance *           | -                                                                                                                                                  | -     |
|                              |                                                                  |              | cloud Connection *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      |       |

| Action                     | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                 | Alias |
|----------------------------|---------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                            |                                                               |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">cc:VpcId</a></li> <li>• <a href="#">cc:VirtualGatewayId</a></li> <li>• <a href="#">cc:EnterpriseRouterId</a></li> </ul> |       |
| cc:networkInstances:delete | Grants permission to remove a network instance.               | Write        | networkInstance *           | <ul style="list-style-type: none"> <li>• <a href="#">cc:VpcId</a></li> <li>• <a href="#">cc:VirtualGatewayId</a></li> <li>• <a href="#">cc:EnterpriseRouterId</a></li> </ul>                                                  | -     |
|                            |                                                               |              | cloudConnection *           | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                 |       |
|                            |                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                         |       |
| cc:networkInstances:update | Grants permission to update a network instance.               | Write        | networkInstance *           | <ul style="list-style-type: none"> <li>• <a href="#">cc:VpcId</a></li> <li>• <a href="#">cc:VirtualGatewayId</a></li> <li>• <a href="#">cc:EnterpriseRouterId</a></li> </ul>                                                  | -     |
|                            |                                                               |              | cloudConnection *           | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                 |       |
|                            |                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                         |       |
| cc:networkInstances:get    | Grants permission to query the details of a network instance. | Read         | networkInstance *           | -                                                                                                                                                                                                                             | -     |
|                            |                                                               |              | cloudConnection *           | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                 |       |



| Action                      | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|-----------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                             |                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| cc:networkInstances:list    | Grants permission to query the network instances.              | List         | networkInstance *           | -                                                                                                                                                                                      | -     |
| cc:bandwidthPackages:create | Grants permission to create a bandwidth package.               | Write        | bandwidthPackage *          | -                                                                                                                                                                                      | -     |
|                             |                                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| cc:bandwidthPackages:delete | Grants permission to delete a bandwidth package.               | Write        | bandwidthPackage *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| cc:bandwidthPackages:update | Grants permission to update a bandwidth package.               | Write        | bandwidthPackage *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| cc:bandwidthPackages:get    | Grants permission to query the details of a bandwidth package. | Read         | bandwidthPackage *          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |

| Action                          | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cc:bandwidth Packages:list      | Grants permission to query the bandwidth packages.                   | List         | band width Package *        | -                                                                                                                                                  | -     |
| cc:bandwidth Packages:tag       | Grants permission to add tags to a bandwidth package.                | Tagging      | band width Package *        | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                 |                                                                      |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| cc:bandwidth Packages:untag     | Grants permission to delete tags from a bandwidth package.           | Tagging      | band width Package *        | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                 |                                                                      |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| cc:bandwidth Packages:listTags  | Grants permission to query the tags added to a bandwidth package.    | List         | band width Package *        | -                                                                                                                                                  | -     |
| cc:bandwidth Packages:associate | Grants permission to bind a bandwidth package to a cloud connection. | Write        | band width Package *        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | -     |
|                                 |                                                                      |              | cloud Connection *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      |       |

| Action                           | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                          | Alias |
|----------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                  |                                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                  |       |
| cc:bandwidth Packages:dissociate | Grants permission to unbind a bandwidth package from a cloud connection. | Write        | bandwidth Package *         | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                          | -     |
|                                  |                                                                          |              | cloud Connection *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                          |       |
|                                  |                                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                  |       |
| cc:interRegion Bandwidths:create | Grants permission to assign an inter-region bandwidth.                   | Write        | interRegion Bandwidth *     | -                                                                                                                                      | -     |
|                                  |                                                                          |              | cloud Connection *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                          |       |
|                                  |                                                                          |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">cc:BandwidthPackageId</a></li> </ul> |       |
| cc:interRegion Bandwidths:delete | Grants permission to delete an inter-region bandwidth.                   | Write        | interRegion Bandwidth *     | <a href="#">cc:BandwidthPackageId</a>                                                                                                  | -     |
|                                  |                                                                          |              | cloud Connection *          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                          |       |
|                                  |                                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                  |       |

| Action                          | Description                                                          | Access Level | Resource Type (*: required) | Condition Key           | Alias |
|---------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|-------------------------|-------|
| cc:interRegionBandwidths:update | Grants permission to modify an inter-region bandwidth.               | Write        | interRegionBandwidth*       | cc:BandwidthPackageId   | -     |
|                                 |                                                                      |              | cloudConnection*            | g:ResourceTag/<tag-key> |       |
|                                 |                                                                      |              | -                           | g:EnterpriseProjectId   |       |
| cc:interRegionBandwidths:get    | Grants permission to query the details of an inter-region bandwidth. | Read         | interRegionBandwidth*       | -                       | -     |
|                                 |                                                                      |              | cloudConnection*            | g:ResourceTag/<tag-key> |       |
|                                 |                                                                      |              | -                           | g:EnterpriseProjectId   |       |
| cc:interRegionBandwidths:list   | Grants permission to query the inter-region bandwidths.              | List         | interRegionBandwidth*       | -                       | -     |
| cc:cloudConnectionRoutes:get    | Grants permission to query the details of a cloud connection route.  | Read         | -                           | -                       | -     |
| cc:cloudConnectionRoutes:list   | Grants permission to query the cloud connection routes.              | List         | -                           | -                       | -     |

| Action                  | Description                                                                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| cc:authorisation:create | Grants permission to allow other accounts to load the VPCs in your account to their cloud connections.                                | Write        | -                           | -             | -     |
| cc:authorisation:delete | Grants permission to stop allowing other accounts to load the VPCs in your account to their cloud connections.                        | Write        | -                           | -             | -     |
| cc:authorisation:update | Grants permission to update the authorization that allows other accounts to load the VPCs in your account to their cloud connections. | Write        | -                           | -             | -     |
| cc:authorisation:list   | Grants permission to query the VPCs that are allowed to be loaded to the cloud connections in other accounts.                         | List         | -                           | -             | -     |

| Action                           | Description                                                                                              | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------|----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| cc:authorisation:listPermissions | Grants permission to query the VPCs that other accounts allow you to load to your cloud connection.      | List         | -                           | -             | -     |
| cc:crossBorderConsent:show       | Grants permission to query the explicit consent for cross-border transfer of personal data.              | Read         | -                           | -             | -     |
| cc:crossBorderConsent:create     | Grants permission to allow users to express explicit consent for cross-border transfer of personal data. | Write        | -                           | -             | -     |
| cc:quota:list                    | Grants permission to query the quotas.                                                                   | List         | -                           | -             | -     |
| cc:capability:list               | Grants permission to query the capabilities of a cloud connection, central network, and site network.    | List         | -                           | -             | -     |

| Action                   | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                    | Alias |
|--------------------------|--------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cc:centralNetwork:create | Grants permission to create a central network.               | Write        | centralNetwork*             | -                                                                                                                                                                                                                                                | -     |
|                          |                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">cc:MultipleEnterpriseRouterIds</a></li> </ul> |       |
| cc:centralNetwork:delete | Grants permission to delete a central network.               | Write        | centralNetwork*             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                               | -     |
| cc:centralNetwork:update | Grants permission to update a central network.               | Write        | centralNetwork*             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                               | -     |
|                          |                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                            |       |
| cc:centralNetwork:get    | Grants permission to query the details of a central network. | Read         | centralNetwork*             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                               | -     |

| Action                         | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cc:centralNetwork:list         | Grants permission to query the central networks.                | List         | centralNetwork*             | -                                                                                                                                                  | -     |
| cc:centralNetwork:tag          | Grants permission to add tags to a central network.             | Tagging      | centralNetwork*             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| cc:centralNetwork:unTag        | Grants permission to delete tags from a central network.        | Tagging      | centralNetwork*             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                                |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |
| cc:centralNetwork:listTags     | Grants permission to query the tags added to a central network. | List         | centralNetwork*             | -                                                                                                                                                  | -     |
| cc:centralNetwork:createPolicy | Grants permission to add a policy to a central network.         | Write        | centralNetwork*             | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |



| Action                            | Description                                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias |
|-----------------------------------|------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
|                                   |                                                                                          |              | -                           | cc:MultipleEnterpriseRouteIds                                                                                  |       |
| cc:centralNetwork:applyPolicy     | Grants permission to apply a policy to a central network.                                | Write        | centralNetwork*             | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| cc:centralNetwork:deletePolicy    | Grants permission to delete a policy from a central network.                             | Write        | centralNetwork*             | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| cc:centralNetwork:listPolicies    | Grants permission to query the central network policies.                                 | List         | centralNetwork*             | -                                                                                                              | -     |
| cc:centralNetwork:listChangeSet   | Grants permission to query the changes between the current policy and an applied policy. | List         | centralNetwork*             | -                                                                                                              | -     |
| cc:centralNetwork:listConnections | Grants permission to query the central network connections.                              | List         | centralNetwork*             | -                                                                                                              | -     |

| Action                                    | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                        | Alias |
|-------------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------|
| cc:centralNetwork:updateConnection        | Grants permission to update a central network connection.                           | Write        | centralNetwork*             | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>                       | -     |
|                                           |                                                                                     |              | -                           | cc:GlobalConnectionBandwidthId                                                                                                       |       |
| cc:centralNetworkAttachment:createGateway | Grants permission to add a global DC gateway to a central network as an attachment. | Write        | centralNetworkAttachment*   | -                                                                                                                                    | -     |
|                                           |                                                                                     |              | centralNetwork*             | g:ResourceTag/<tag-key>                                                                                                              |       |
|                                           |                                                                                     |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>cc:EnterpriseRouterId</li> <li>cc:GlobalDCGatewayId</li> </ul> |       |
| cc:centralNetworkAttachment:updateGateway | Grants permission to update a global DC gateway on a central network.               | Write        | centralNetworkAttachment*   | <ul style="list-style-type: none"> <li>cc:GlobalDCGatewayId</li> <li>cc:EnterpriseRouterId</li> </ul>                                | -     |
|                                           |                                                                                     |              | centralNetwork*             | g:ResourceTag/<tag-key>                                                                                                              |       |
|                                           |                                                                                     |              | -                           | g:EnterpriseProjectId                                                                                                                |       |

| Action                                         | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                   | Alias |
|------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------|-------|
| cc:centralNetworkAttachment:getGdgw            | Grants permission to query the details of a global DC gateway on a central network.              | Read         | centralNetworkAttachment*   | <ul style="list-style-type: none"> <li>cc:GlobalDcGatewayId</li> <li>cc:EnterpriseRouterId</li> </ul>           | -     |
|                                                |                                                                                                  |              | centralNetwork*             | g:ResourceTag/<tag-key>                                                                                         |       |
|                                                |                                                                                                  |              | -                           | g:EnterpriseProjectId                                                                                           |       |
| cc:centralNetworkAttachment:listGdgws          | Grants permission to query the global DC gateways on a central network.                          | List         | centralNetworkAttachment*   | -                                                                                                               | -     |
|                                                |                                                                                                  |              | centralNetwork*             | g:ResourceTag/<tag-key>                                                                                         |       |
|                                                |                                                                                                  |              | -                           | g:EnterpriseProjectId                                                                                           |       |
| cc:centralNetworkAttachment:createErRouteTable | Grants permission to add an enterprise router route table to a central network as an attachment. | Write        | centralNetworkAttachment*   | -                                                                                                               | -     |
|                                                |                                                                                                  |              | centralNetwork*             | g:ResourceTag/<tag-key>                                                                                         |       |
|                                                |                                                                                                  |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>cc:MultipleEnterpriseRouterIds</li> </ul> |       |

| Action                                         | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key                 | Alias |
|------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------|-------|
| cc:centralNetworkAttachment:updateErRouteTable | Grants permission to update an enterprise router route table on a central network.               | Write        | centralNetworkAttachment*   | cc:MultipleEnterpriseRouteIds | -     |
|                                                |                                                                                                  |              | centralNetwork*             | g:ResourceTag/<tag-key>       |       |
|                                                |                                                                                                  |              | -                           | g:EnterpriseProjectId         |       |
| cc:centralNetworkAttachment:getErRouteTable    | Grants permission to query the details of an enterprise router route table on a central network. | Read         | centralNetworkAttachment*   | cc:MultipleEnterpriseRouteIds | -     |
|                                                |                                                                                                  |              | centralNetwork*             | g:ResourceTag/<tag-key>       |       |
|                                                |                                                                                                  |              | -                           | g:EnterpriseProjectId         |       |
| cc:centralNetworkAttachment:listErRouteTables  | Grants permission to query the enterprise router route tables on a central network.              | List         | centralNetworkAttachment*   | -                             | -     |
|                                                |                                                                                                  |              | centralNetwork*             | g:ResourceTag/<tag-key>       |       |
|                                                |                                                                                                  |              | -                           | g:EnterpriseProjectId         |       |

| Action                             | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias |
|------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cc:centralNetworkAttachment:delete | Grants permission to delete an attachment from a central network. | Write        | centralNetworkAttachment*   | <ul style="list-style-type: none"> <li>cc:GlobalIDcGatewayId</li> <li>cc:EnterpriseRouterId</li> <li>cc:MultipleEnterpriseRouterIds</li> </ul> | -     |
|                                    |                                                                   |              | centralNetwork*             | g:ResourceTag/<tag-key>                                                                                                                        |       |
|                                    |                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                                          |       |
| cc:centralNetworkAttachment:list   | Grants permission to query the central network attachments.       | List         | centralNetworkAttachment*   | -                                                                                                                                              | -     |
|                                    |                                                                   |              | centralNetwork*             | g:ResourceTag/<tag-key>                                                                                                                        |       |
|                                    |                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                                          |       |
| cc:siteNetwork:createP2P           | Grants permission to create a P2P site network.                   | Write        | siteNetwork*                | -                                                                                                                                              | -     |
| cc:siteNetwork:list                | Grants permission to query the site networks.                     | List         | siteNetwork*                | -                                                                                                                                              | -     |
| cc:siteNetwork:get                 | Grants permission to query the details of a site network.         | Read         | siteNetwork*                | -                                                                                                                                              | -     |

| Action                               | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                | Alias                |
|--------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|------------------------------|----------------------|
| cc:siteNetwork:update                | Grants permission to update a site network.                  | Write        | siteNetwork *               | -                            | -                    |
| cc:siteNetwork:delete                | Grants permission to delete a site network.                  | Write        | siteNetwork *               | -                            | -                    |
| cc:siteNetwork:disassociateBandwidth | Grants permission to unbind a site network bandwidth.        | Write        | siteNetwork *               | -                            | -                    |
| cc:siteNetwork:associateBandwidth    | Grants permission to bind a site network bandwidth.          | Write        | siteNetwork *               | -                            | -                    |
| cc:siteNetwork:updateBandwidthSize   | Grants permission to modify the site network bandwidth size. | Write        | siteNetwork *               | -                            | -                    |
| cc:siteNetwork:updateBandwidth       | Grants permission to change the site network bandwidth.      | Write        | siteNetwork *               | -                            | -                    |
| cc:gcbandwidths:list                 | Grants permission to query global connection bandwidths.     | List         | gcbandwidth *               | -                            | cc:gcbandwidths:list |
|                                      |                                                              |              | -                           | <b>g:EnterpriseProjectId</b> |                      |

| Action                      | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                   |
|-----------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| cc:gcbandwidth:get          | Grants permission to query the details of a global connection bandwidth.  | Read         | gcbandwidth *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | cc:gcbandwidthhs:get    |
| cc:gcbandwidth:create       | Grants permission to create a global connection bandwidth.                | Write        | gcbandwidth *               | -                                                                                                                                                                                      | cc:gcbandwidthhs:create |
|                             |                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                         |
| cc:gcbandwidth:update       | Grants permission to update a global connection bandwidth.                | Write        | gcbandwidth *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | cc:gcbandwidthhs:update |
| cc:gcbandwidth:delete       | Grants permission to delete a global connection bandwidth.                | Write        | gcbandwidth *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | cc:gcbandwidthhs:delete |
| cc:gcbandwidth:getRelations | Grants permission to query global connection bandwidth binding relations. | Read         | gcbandwidth *               | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | cc:gcbandwidthhs:get    |

| Action                              | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                             | Alias                      |
|-------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| cc:gcbandwidth:associateInstance    | Grants permission to bind a global connection bandwidth to an instance.                 | Write        | gcbandwidth *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                        | cc:gcbandwidths:update     |
|                                     |                                                                                         |              | -                           | <a href="#">cc:gcbAssociateResourceType</a>                                                                                                                                                               |                            |
| cc:gcbandwidth:disassociateInstance | Grants permission to unbind a global connection bandwidth from an instance.             | Write        | gcbandwidth *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">cc:gcbAssociateResourceType</a></li> </ul> | cc:gcbandwidths:update     |
| cc:gcbandwidth:listSupportBinding   | Grants permission to query global connection bandwidths that can be bound to instances. | List         | gcbandwidth *               | -                                                                                                                                                                                                         | cc:gcbandwidths:list       |
|                                     |                                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                     |                            |
| cc:gcbandwidth:listTags             | Grants permission to query tags of a global connection bandwidth.                       | List         | gcbandwidth *               | -                                                                                                                                                                                                         | cc:gcbandwidths:listByTag  |
| cc:gcbandwidth:tag                  | Grants permission to add tags to a global connection bandwidth.                         | Tagging      | gcbandwidth *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                        | cc:gcbandwidths:createTags |



| Action               | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                      |
|----------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
|                      |                                                                      |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                            |
| cc:gcbandwidth:unTag | Grants permission to delete tags from a global connection bandwidth. | Tagging      | gcbandwidth *               | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | cc:gcbandwidths:deleteTags |
|                      |                                                                      |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |                            |

Each API of CC usually supports one or more actions. [Table 3-65](#) lists the supported actions and dependencies.

**Table 3-65** Actions and dependencies supported by CC APIs

| API                                                 | Action                     | Dependencies |
|-----------------------------------------------------|----------------------------|--------------|
| POST /v3/{domain_id}/ccaas/cloud-connections        | cc:cloudConnections:create | -            |
| PUT /v3/{domain_id}/ccaas/cloud-connections/{id}    | cc:cloudConnections:update | -            |
| DELETE /v3/{domain_id}/ccaas/cloud-connections/{id} | cc:cloudConnections:delete | -            |
| GET /v3/{domain_id}/ccaas/cloud-connections/{id}    | cc:cloudConnections:get    | -            |
| GET /v3/{domain_id}/ccaas/cloud-connections         | cc:cloudConnections:list   | -            |

| API                                                     | Action                       | Dependencies |
|---------------------------------------------------------|------------------------------|--------------|
| POST /v3/{domain_id}/ccaas/cloud-connections/filter     | cc:cloudConnections:list     | -            |
| POST /v3/{domain_id}/ccaas/cloud-connections/{id}/tag   | cc:cloudConnections:tag      | -            |
| POST /v3/{domain_id}/ccaas/cloud-connections/{id}/untag | cc:cloudConnections:unTag    | -            |
| GET /v3/{domain_id}/ccaas/cloud-connections/tags        | cc:cloudConnections:listTags | -            |
| POST /v3/{domain_id}/ccaas/network-instances            | cc:networkInstances:create   | -            |
| PUT /v3/{domain_id}/ccaas/network-instances/{id}        | cc:networkInstances:update   | -            |
| DELETE /v3/{domain_id}/ccaas/network-instances/{id}     | cc:networkInstances:delete   | -            |
| GET /v3/{domain_id}/ccaas/network-instances/{id}        | cc:networkInstances:get      | -            |
| GET /v3/{domain_id}/ccaas/network-instances             | cc:networkInstances:list     | -            |
| POST /v3/{domain_id}/ccaas/bandwidth-packages           | cc:bandwidthPackages:create  | -            |
| PUT /v3/{domain_id}/ccaas/bandwidth-packages/{id}       | cc:bandwidthPackages:update  | -            |

| API                                                             | Action                            | Dependencies |
|-----------------------------------------------------------------|-----------------------------------|--------------|
| DELETE /v3/{domain_id}/ccaas/bandwidth-packages/{id}            | cc:bandwidthPackages:delete       | -            |
| GET /v3/{domain_id}/ccaas/bandwidth-packages/{id}               | cc:bandwidthPackages:get          | -            |
| GET /v3/{domain_id}/ccaas/bandwidth-packages                    | cc:bandwidthPackages:list         | -            |
| POST /v3/{domain_id}/ccaas/bandwidth-packages/filter            | cc:bandwidthPackages:list         | -            |
| POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/tag          | cc:bandwidthPackages:tag          | -            |
| POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/untag        | cc:bandwidthPackages:unTag        | -            |
| GET /v3/{domain_id}/ccaas/bandwidth-packages/tags               | cc:bandwidthPackages:listTags     | -            |
| POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/associate    | cc:bandwidthPackages:associate    | -            |
| POST /v3/{domain_id}/ccaas/bandwidth-packages/{id}/disassociate | cc:bandwidthPackages:disassociate | -            |
| GET /v3/{domain_id}/ccaas/bandwidth-packages/free-packages      | cc:bandwidthPackages:list         | -            |

| API                                                             | Action                          | Dependencies |
|-----------------------------------------------------------------|---------------------------------|--------------|
| POST /v3/{domain_id}/ccaas/bandwidth-packages/orders/{order_id} | cc:bandwidthPackages:create     | -            |
| PUT /v3/{domain_id}/ccaas/bandwidth-packages/orders/{order_id}  | cc:bandwidthPackages:update     | -            |
| POST /v3/{domain_id}/ccaas/inter-region-bandwidths              | cc:interRegionBandwidths:create | -            |
| PUT /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}          | cc:interRegionBandwidths:update | -            |
| DELETE /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}       | cc:interRegionBandwidths:delete | -            |
| GET /v3/{domain_id}/ccaas/inter-region-bandwidths/{id}          | cc:interRegionBandwidths:get    | -            |
| GET /v3/{domain_id}/ccaas/inter-region-bandwidths               | cc:interRegionBandwidths:list   | -            |
| GET /v3/{domain_id}/ccaas/cloud-connection-routes/{id}          | cc:cloudConnectionRoutes:get    | -            |
| GET /v3/{domain_id}/ccaas/cloud-connection-routes               | cc:cloudConnectionRoutes:list   | -            |
| POST /v3/{domain_id}/ccaas/authorisations                       | cc:authorisation:create         | -            |

| API                                              | Action                           | Dependencies                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v3/{domain_id}/ccaas/authorisations/{id} | cc:authorisation:delete          | -                                                                                                                                                                                                                                                                                                                                                            |
| PUT /v3/{domain_id}/ccaas/authorisations/{id}    | cc:authorisation:update          | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/ccaas/authorisations         | cc:authorisation:list            | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/ccaas/permissions            | cc:authorisation:listPermissions | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/ccaas/quotas                 | cc:quota:list                    | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/quotas                   | cc:quota:list                    | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/ccaas/capabilities           | cc:capability:list               | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/capabilities             | cc:capability:list               | -                                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/gcn/central-networks        | cc:centralNetwork:create         | <ul style="list-style-type: none"> <li>• er:instances:get</li> <li>• er:routeTables:get</li> <li>• er:routeTables:listPropagations</li> <li>• er:routeTables:enablePropagation</li> <li>• er:routeTables:disablePropagation</li> <li>• er:routeTables:listAssociations</li> <li>• er:routeTables:associate</li> <li>• er:routeTables:disassociate</li> </ul> |

| API                                                                  | Action                   | Dependencies                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v3/{domain_id}/gcn/central-networks/{central_network_id}     | cc:centralNetwork:delete | <ul style="list-style-type: none"> <li>er:instances:get</li> <li>er:routeTables:get</li> <li>er:routeTables:listPropagations</li> <li>er:routeTables:enablePropagation</li> <li>er:routeTables:disablePropagation</li> <li>er:routeTables:listAssociations</li> <li>er:routeTables:associate</li> <li>er:routeTables:disassociate</li> </ul> |
| PUT /v3/{domain_id}/gcn/central-networks/{central_network_id}        | cc:centralNetwork:update | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-networks/{central_network_id}        | cc:centralNetwork:get    | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-networks                             | cc:centralNetwork:list   | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/gcn/central-networks/filter                     | cc:centralNetwork:list   | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/gcn/central-networks/{central_network_id}/tag   | cc:centralNetwork:tag    | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/gcn/central-networks/{central_network_id}/untag | cc:centralNetwork:unTag  | -                                                                                                                                                                                                                                                                                                                                            |

| API                                                                                          | Action                            | Dependencies                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v3/{domain_id}/gcn/central-networks/tags                                                | cc:centralNetwork:listTags        | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/gcn/central-network/{central_network_id}/policies                       | cc:centralNetwork:createPolicy    | <ul style="list-style-type: none"> <li>er:instances:get</li> <li>er:routeTables:get</li> </ul>                                                                                                                                                                                                                                               |
| POST /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}/apply     | cc:centralNetwork:applyPolicy     | <ul style="list-style-type: none"> <li>er:instances:get</li> <li>er:routeTables:get</li> <li>er:routeTables:listPropagations</li> <li>er:routeTables:enablePropagation</li> <li>er:routeTables:disablePropagation</li> <li>er:routeTables:listAssociations</li> <li>er:routeTables:associate</li> <li>er:routeTables:disassociate</li> </ul> |
| DELETE /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}         | cc:centralNetwork:deletePolicy    | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/policies                        | cc:centralNetwork:listPolicies    | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}/change-set | cc:centralNetwork:listChangeSet   | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/connections                     | cc:centralNetwork:listConnections | -                                                                                                                                                                                                                                                                                                                                            |

| API                                                                                                | Action                                 | Dependencies                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/connections/{connection_id}           | cc:centralNetwork:updateConnection     | -                                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments                     | cc:centralNetworkAttachment:createGdgw | <ul style="list-style-type: none"> <li>• er:instances:get</li> <li>• er:routeTables:get</li> <li>• er:routeTables:listPropagations</li> <li>• er:routeTables:enablePropagation</li> <li>• er:routeTables:disablePropagation</li> <li>• er:routeTables:listAssociations</li> <li>• er:routeTables:associate</li> <li>• er:routeTables:disassociate</li> </ul> |
| PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments/{gdgw_attachment_id} | cc:centralNetworkAttachment:updateGdgw | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments/{gdgw_attachment_id} | cc:centralNetworkAttachment:getGdgw    | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments                      | cc:centralNetworkAttachment:listGdgws  | -                                                                                                                                                                                                                                                                                                                                                            |



| API                                                                                                                    | Action                                         | Dependencies                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments                               | cc:centralNetworkAttachment:createErRouteTable | <ul style="list-style-type: none"> <li>• er:instances:get</li> <li>• er:routeTables:get</li> <li>• er:routeTables:listPropagations</li> <li>• er:routeTables:enablePropagation</li> <li>• er:routeTables:disablePropagation</li> <li>• er:routeTables:listAssociations</li> <li>• er:routeTables:associate</li> <li>• er:routeTables:disassociate</li> </ul> |
| PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments/{er_route_table_attachment_id} | cc:centralNetworkAttachment:updateErRouteTable | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments/{er_route_table_attachment_id} | cc:centralNetworkAttachment:getErRouteTable    | -                                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments                                | cc:centralNetworkAttachment:listErRouteTables  | -                                                                                                                                                                                                                                                                                                                                                            |

| API                                                                                         | Action                             | Dependencies                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments/{attachment_id} | cc:centralNetworkAttachment:delete | <ul style="list-style-type: none"> <li>er:instances:get</li> <li>er:routeTables:get</li> <li>er:routeTables:listPropagations</li> <li>er:routeTables:enablePropagation</li> <li>er:routeTables:disablePropagation</li> <li>er:routeTables:listAssociations</li> <li>er:routeTables:associate</li> <li>er:routeTables:disassociate</li> </ul> |
| GET /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments                    | cc:centralNetworkAttachment:list   | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/ccaas/domain-cross-border-consents                                      | cc:crossBorderConsent:show         | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/ccaas/domain-cross-border-consents                                     | cc:crossBorderConsent:create       | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v3/{domain_id}/dcaas/p2p-site-networks                                                | cc:siteNetwork:createP2P           | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/dcaas/site-networks                                                     | cc:siteNetwork:list                | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v3/{domain_id}/dcaas/site-networks/{site_network_id}                                   | cc:siteNetwork:get                 | -                                                                                                                                                                                                                                                                                                                                            |
| PUT /v3/{domain_id}/dcaas/site-networks/{site_network_id}                                   | cc:siteNetwork:update              | -                                                                                                                                                                                                                                                                                                                                            |

| API                                                                                                              | Action                               | Dependencies |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| DELETE /v3/{domain_id}/dcaas/site-networks/{site_network_id}                                                     | cc:siteNetwork:delete                | -            |
| POST /v3/{domain_id}/dcaas/site-network/{site_network_id}/connections/{site_connection_id}/disassociate          | cc:siteNetwork:disassociateBandwidth | -            |
| POST /v3/{domain_id}/dcaas/site-network/{site_network_id}/connections/{site_connection_id}/associate             | cc:siteNetwork:associateBandwidth    | -            |
| POST /v3/{domain_id}/dcaas/site-network/{site_network_id}/connections/{site_connection_id}/update-bandwidth-size | cc:siteNetwork:updateBandwidthSize   | -            |
| POST /v3/{domain_id}/dcaas/site-network/{site_network_id}/connections/{site_connection_id}/update-bandwidth      | cc:siteNetwork:updateBandwidth       | -            |
| GET /v3/{domain_id}/dcaas/site-network/capabilities                                                              | cc:capability:list                   | -            |
| GET /v3/{domain_id}/dcaas/site-network/quotas                                                                    | cc:quota:list                        | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-66](#), the resource URN must be

specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CC.

**Table 3-66** Resource types supported by CC

| Resource Type            | URN                                                                       |
|--------------------------|---------------------------------------------------------------------------|
| cloudConnection          | cc::<account-id>:cloudConnection:<cloud-connection-id>                    |
| gcbandwidth              | cc::<account-id>:gcbandwidth:<gcbandwidth-id>                             |
| interRegionBandwidth     | cc::<account-id>:interRegionBandwidth:<inter-region-bandwidth-id>         |
| networkInstance          | cc::<account-id>:networkInstance:<network-instance-id>                    |
| siteNetwork              | cc::<account-id>:siteNetwork:<site-network-id>                            |
| bandwidthPackage         | cc::<account-id>:bandwidthPackage:<bandwidth-package-id>                  |
| centralNetwork           | cc::<account-id>:centralNetwork:<central-network-id>                      |
| centralNetworkAttachment | cc::<account-id>:centralNetworkAttachment:<central-network-attachment-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, cc) apply only to operations of the xx service. For details, see **Table 3-67**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have

multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.

- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by CC

The following table lists the condition keys that you can define in identity policies for CC. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-67** Service-specific condition keys supported by CC

| Service-specific Condition Key                  | Type   | Single-valued/<br>Multivalued | Description                                                      |
|-------------------------------------------------|--------|-------------------------------|------------------------------------------------------------------|
| <a href="#">cc:VpcId</a>                        | string | Single-valued                 | Filters access by VPC ID.                                        |
| <a href="#">cc:VirtualGatewayId</a>             | string | Single-valued                 | Filters access by virtual gateway ID.                            |
| <a href="#">cc:EnterpriseRouterId</a>           | string | Single-valued                 | Filters access by enterprise router ID.                          |
| <a href="#">cc:MultipleEnterpriseRouterIds</a>  | string | Multivalued                   | Filters access by enterprise router IDs.                         |
| <a href="#">cc:BandwidthPackageId</a>           | string | Single-valued                 | Filters access by bandwidth package ID.                          |
| <a href="#">cc:GlobalConnection-BandwidthId</a> | string | Single-valued                 | Filters access by global connection bandwidth ID.                |
| <a href="#">cc:GlobalDcGatewayId</a>            | string | Single-valued                 | Filters access by global DC gateway ID.                          |
| <a href="#">cc:gcbAssociateResourceType</a>     | string | Single-valued                 | Filters access to global connection bandwidths by resource type. |

### Examples of Condition Keys

- `cc:VpcId`  
For example, Filters access to network instances by VPC ID.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:networkInstances:create",
        "cc:networkInstances:delete",
        "cc:networkInstances:update"
      ],
      "Condition": {
        "StringEquals": {
          "cc:VpcId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- cc:VirtualGatewayId

For example, Filters access to network instances by virtual gateway ID.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:networkInstances:create",
        "cc:networkInstances:delete",
        "cc:networkInstances:update"
      ],
      "Condition": {
        "StringEquals": {
          "cc:VirtualGatewayId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- cc:EnterpriseRouterId

For example, Filters access to global DC gateways attached to a central network by enterprise router ID.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetworkAttachment:createGdgw",
        "cc:centralNetworkAttachment:updateGdgw",
        "cc:centralNetworkAttachment:getGdgw",
        "cc:centralNetworkAttachment:delete"
      ],
      "Condition": {
        "StringEquals": {
          "cc:EnterpriseRouterId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- **cc:MultipleEnterpriseRouterIds**

For example, Filters access to central networks and enterprise router route table attachments by enterprise router IDs.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetwork:create",
        "cc:centralNetwork:createPolicy",
        "cc:centralNetworkAttachment:createErRouteTable",
        "cc:centralNetworkAttachment:updateErRouteTable",
        "cc:centralNetworkAttachment:getErRouteTable",
        "cc:centralNetworkAttachment:delete"
      ],
      "Condition": {
        "StringEquals": {
          "cc:MultipleEnterpriseRouterIds": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- **cc:BandwidthPackageId**

For example, Filters access to inter-region bandwidths by bandwidth package ID.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:interRegionBandwidths:create",
        "cc:interRegionBandwidths:delete",
        "cc:interRegionBandwidths:update"
      ],
      "Condition": {
        "StringEquals": {
          "cc:BandwidthPackageId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

- **cc:GlobalConnectionBandwidthId**

For example, Filters access to central network connections by global connection bandwidth ID.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetwork:updateConnection"
      ],
      "Condition": {
        "StringEquals": {
          "cc:GlobalConnectionBandwidthId": [
            "xxx"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
}
]
}

```

- **cc:GlobalDcGatewayId**

For example, Filters access to global DC gateways attached to a central network by global DC gateway ID.

```

{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetworkAttachment:createGdgw",
        "cc:centralNetworkAttachment:updateGdgw",
        "cc:centralNetworkAttachment:getGdgw",
        "cc:centralNetworkAttachment:delete"
      ],
      "Condition": {
        "StringEquals": {
          "cc:GlobalDcGatewayId": [
            "xxx"
          ]
        }
      }
    }
  ]
}

```

- **cc:gcbAssociateResourceType**

For example, Filters access to the resource binding API or resource unbinding API by the type of the resource bound to the global connection bandwidth.

```

{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:gcbandwidth:associateInstance",
        "cc:gcbandwidth:disassociateInstance",
      ],
      "Condition": {
        "StringEquals": {
          "cc:gcbAssociateResourceType": [
            "xxx"
          ]
        }
      }
    }
  ]
}

```

### 3.3.9 Elastic Load Balance

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational



unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by ELB, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by ELB, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for ELB.

**Table 3-68** Actions supported by ELB

| Action                      | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                | Alias                 |
|-----------------------------|---------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| elb:flavors:show            | Grants permission to show flavor.           | Read         | flavor *                    | -                                                                                                                            | elb:flavors:get       |
| elb:flavors:list            | Grants permission to list flavors.          | List         | flavor *                    | -                                                                                                                            | -                     |
| elb:quotas:list             | Grants permission to list quotas.           | List         | -                           | -                                                                                                                            | -                     |
| elb:quotas:show             | Grants permission to show resource quota.   | Read         | -                           | -                                                                                                                            | elb:quotas:get        |
| elb:availability-zones:list | Grants permission to list az.               | List         | availability Zone *         | -                                                                                                                            | -                     |
|                             |                                             |              | -                           | <b>g:EnterpriseProjectId</b>                                                                                                 |                       |
| elb:loadbalancers:list      | Grants permission to list loadbalancer.     | List         | loadbalancer *              | -                                                                                                                            | -                     |
|                             |                                             |              | -                           | <b>g:EnterpriseProjectId</b>                                                                                                 |                       |
| elb:loadbalancers:show      | Grants permission to get loadbalancer info. | Read         | loadbalancer *              | <ul style="list-style-type: none"> <li><b>g:ResourceTag/&lt;tag-key&gt;</b></li> <li><b>g:EnterpriseProjectId</b></li> </ul> | elb:loadbalancers:get |
| elb:loadbalancers:create    | Grants permission to create loadbalancer.   | Write        | loadbalancer *              | -                                                                                                                            | -                     |
|                             |                                             |              | subnet                      | -                                                                                                                            |                       |

| Action                   | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                            | Alias                 |
|--------------------------|-------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                          |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">elb:AssociatePublicips</a></li> </ul> |                       |
| elb:loadbalancers:update | Grants permission to update loadbalancer. | Write        | subnet                      | -                                                                                                                                                                                                                                        | elb:loadbalancers:put |
|                          |                                           |              | loadbalancer *              | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                       |                       |
|                          |                                           |              | -                           | <a href="#">elb:AssociatePublicips</a>                                                                                                                                                                                                   |                       |
| elb:loadbalancers:delete | Grants permission to delete loadbalancer. | Write        | loadbalancer *              | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                       | -                     |
| elb:listeners:create     | Grants permission to create listener.     | Write        | listener *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                    | -                     |
|                          |                                           |              | loadbalancer *              | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                       |                       |
|                          |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                    |                       |

| Action                | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                | Alias                |
|-----------------------|--------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| elb:listeners:update  | Grants permission to update listener.      | Write        | listener *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">elb:UpdateListenerGroup</a></li> <li>• <a href="#">elb:OnlyUpdateListenerGroup</a></li> </ul> | elb:listeners:put    |
| elb:listeners:list    | Grants permission to list listener.        | List         | listener *                  | -                                                                                                                                                                                                                                                            | -                    |
|                       |                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                        |                      |
| elb:listeners:show    | Grants permission to get listener.         | Read         | listener *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                           | elb:listeners:get    |
| elb:listeners:delete  | Grants permission to delete listener.      | Write        | listener *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                           | -                    |
| elb:certificates:list | Grants permission to list certificate.     | List         | certificate *               | -                                                                                                                                                                                                                                                            | -                    |
|                       |                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                        |                      |
| elb:certificates:show | Grants permission to get certificate info. | Read         | certificate *               | -                                                                                                                                                                                                                                                            | elb:certificates:get |

| Action                             | Description                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|------------------------------------|---------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| elb:certificates:create            | Grants permission to create certificate.          | Write        | certificate *               | -                                     |                        |
|                                    |                                                   |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| elb:certificates:update            | Grants permission to modify certificate.          | Write        | certificate *               | -                                     | elb:certificates:put   |
| elb:certificates:delete            | Grants permission to delete certificate.          | Write        | certificate *               | -                                     | -                      |
| elb:certificates:setPrivateKeyEcho | Grants permission to set private key echo switch. | Write        | -                           | -                                     | -                      |
| elb:certificates:getPrivateKeyEcho | Grants permission to get private key echo switch. | Write        | -                           | -                                     | -                      |
| elb:healthmonitors:create          | Grants permission to create a healthmonitor.      | Write        | healthmonitor *             | <a href="#">g:EnterpriseProjectId</a> |                        |
|                                    |                                                   |              | pool *                      | <a href="#">g:EnterpriseProjectId</a> |                        |
| elb:healthmonitors:update          | Grants permission to modify healthmonitor.        | Write        | healthmonitor *             | <a href="#">g:EnterpriseProjectId</a> | elb:healthmonitors:put |
| elb:healthmonitors:delete          | Grants permission to delete healthmonitor.        | Write        | healthmonitor *             | <a href="#">g:EnterpriseProjectId</a> | -                      |

| Action                            | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                          |
|-----------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------|
| elb:healthmonitors:show           | Grants permission to get healthmonitor.                                   | Read         | healthmonitor *             | <a href="#">g:EnterpriseProjectId</a> | elb:healthmonitors:get         |
| elb:healthmonitors:list           | Grants permission to list healthmonitor.                                  | List         | healthmonitor *             | -                                     | -                              |
|                                   |                                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                |
| elb:ipgroups:list                 | Grants permission to list ipgroups.                                       | List         | ipgroup *                   | -                                     | -                              |
|                                   |                                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                |
| elb:ipgroups:show                 | Grants permission to get ipgroup info.                                    | Read         | ipgroup *                   | -                                     | elb:ipgroups:get               |
| elb:ipgroups:create               | Grants permission to create ipgroup.                                      | Write        | ipgroup *                   | -                                     | -                              |
|                                   |                                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                |
| elb:ipgroups:update               | Grants permission to modify ipgroup.                                      | Write        | ipgroup *                   | -                                     | elb:ipgroups:put               |
| elb:ipgroups:delete               | Grants permission to delete ipgroup.                                      | Write        | ipgroup *                   | -                                     | -                              |
| elb:ipgroups:showRelatedListeners | Grants permission to get listeners associated with the specified ipgroup. | Read         | ipgroup *                   | -                                     | elb:ipgroups:related-listeners |

| Action                | Description                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias              |
|-----------------------|-----------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| elb:l7policies:create | Grants permission to create l7policy.   | Write        | listener *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                  |
|                       |                                         |              | l7policy *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                    |
|                       |                                         |              | pool                        | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                    |
| elb:l7policies:update | Grants permission to modify l7policy.   | Write        | l7policy *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | elb:l7policies:put |
|                       |                                         |              | listener                    | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                    |
|                       |                                         |              | pool                        | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                    |
| elb:l7policies:delete | Grants permission to delete l7policy.   | Write        | l7policy *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                  |
| elb:l7policies:show   | Grants permission to get l7policy info. | Read         | l7policy *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | elb:l7policies:get |
| elb:l7policies:list   | Grants permission to list l7policies.   | List         | l7policy *                  | -                                                                                                                                                  | -                  |
|                       |                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                    |
| elb:l7rules:create    | Grants permission to create l7rule.     | Write        | l7rule *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -                  |
|                       |                                         |              | l7policy *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                              |                    |

| Action              | Description                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias            |
|---------------------|-----------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| elb:l7rules:update  | Grants permission to modify l7rule.     | Write        | l7rule *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | elb:l7rules:put  |
| elb:l7rules:list    | Grants permission to list l7rules.      | List         | l7policy *                  | -                                                                                                                                              | -                |
|                     |                                         |              | l7rule *                    | -                                                                                                                                              |                  |
|                     |                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                  |
| elb:l7rules:show    | Grants permission to get l7rule.        | Read         | l7rule *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | elb:l7rules:get  |
| elb:l7rules:delete  | Grants permission to delete l7rule.     | Write        | l7rule *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -                |
| elb:logtanks:list   | Grants permission to list logtanks.     | List         | logtank *                   | -                                                                                                                                              | -                |
|                     |                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                  |
| elb:logtanks:show   | Grants permission to show logtank info. | Read         | logtank *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | elb:logtanks:get |
| elb:logtanks:create | Grants permission to create logtank.    | Write        | logtank *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -                |
|                     |                                         |              | loadbalancer *              | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |                  |
| elb:logtanks:update | Grants permission to modify logtank.    | Write        | logtank *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | elb:logtanks:put |



| Action              | Description                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias         |
|---------------------|--------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| elb:logtanks:delete | Grants permission to delete logtank. | Write        | logtank *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -             |
| elb:pools:list      | Grants permission to list pool.      | List         | pool *                      | -                                                                                                                                              | -             |
|                     |                                      |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |               |
| elb:pools:show      | Grants permission to get pool.       | Read         | pool *                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | elb:pools:get |
| elb:pools:create    | Grants permission to create pool.    | Write        | loadbalancer                | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -             |
|                     |                                      |              | listener                    | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |               |
|                     |                                      |              | pool *                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |               |
| elb:pools:update    | Grants permission to modify pool.    | Write        | pool *                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | elb:pools:put |
| elb:pools:delete    | Grants permission to delete pool.    | Write        | pool *                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -             |
| elb:members:list    | Grants permission to list member.    | List         | pool                        | -                                                                                                                                              | -             |
|                     |                                      |              | member *                    | -                                                                                                                                              |               |
|                     |                                      |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |               |

| Action                       | Description                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                     |
|------------------------------|----------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------|
| elb:members:show             | Grants permission to get member.             | Read         | member *                    | <a href="#">g:EnterpriseProjectId</a> | elb:members:get           |
| elb:members:create           | Grants permission to create member.          | Write        | member *                    | <a href="#">g:EnterpriseProjectId</a> | -                         |
|                              |                                              |              | pool *                      | <a href="#">g:EnterpriseProjectId</a> |                           |
|                              |                                              |              | subnet                      | -                                     |                           |
| elb:members:update           | Grants permission to modify member.          | Write        | member *                    | <a href="#">g:EnterpriseProjectId</a> | elb:members:put           |
| elb:members:delete           | Grants permission to delete member.          | Write        | member *                    | <a href="#">g:EnterpriseProjectId</a> | -                         |
| elb:security-policies:list   | Grants permission to list security-policies. | List         | securityPolicy *            | -                                     | -                         |
|                              |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                           |
| elb:security-policies:show   | Grants permission to get security-policy.    | Read         | securityPolicy *            | -                                     | elb:security-policies:get |
| elb:security-policies:create | Grants permission to create security-policy. | Write        | securityPolicy *            | -                                     | -                         |
|                              |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                           |
| elb:security-policies:update | Grants permission to modify security-policy. | Write        | securityPolicy *            | -                                     | elb:security-policies:put |

| Action                       | Description                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------|----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| elb:security-policies:delete | Grants permission to delete security-policy. | Write        | securityPolicy *            | -                                                                                                                                                  | -     |
| elb:loadbalancers:export     | Grants permission to export loadbalancers.   | Read         | loadbalancer *              | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| elb:listeners:export         | Grants permission to export listeners.       | Read         | listener *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

Each API of ELB usually supports one or more actions. [Table 3-69](#) lists the supported actions and dependencies.

**Table 3-69** Actions and dependencies supported by ELB APIs

| API                                          | Action           | Dependencies |
|----------------------------------------------|------------------|--------------|
| GET /v3/{project_id}/elb/flavors             | elb:flavors:list | -            |
| GET /v3/{project_id}/elb/flavors/{flavor_id} | elb:flavors:show | -            |
| GET /v3/{project_id}/elb/quotas/details      | elb:quotas:list  | -            |
| GET /v3/{project_id}/elb/quotas              | elb:quotas:show  | -            |

| API                                                                                      | Action                   | Dependencies |
|------------------------------------------------------------------------------------------|--------------------------|--------------|
| POST /v3/{project_id}/elb/loadbalancers                                                  | elb:loadbalancers:create | -            |
| DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}                              | elb:loadbalancers:delete | -            |
| DELETE /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/force-elb                    | elb:loadbalancers:delete | -            |
| GET /v3/{project_id}/elb/loadbalancers                                                   | elb:loadbalancers:list   | -            |
| GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}                                 | elb:loadbalancers:show   | -            |
| GET /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/statuses                        | elb:loadbalancers:show   | -            |
| PUT /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}                                 | elb:loadbalancers:update | -            |
| POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-remove | elb:loadbalancers:update | -            |
| POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-add    | elb:loadbalancers:update | -            |
| POST /v3/{project_id}/elb/ipgroups                                                       | elb:ipgroups:create      | -            |

| API                                                                     | Action                            | Dependencies |
|-------------------------------------------------------------------------|-----------------------------------|--------------|
| DELETE /v3/{project_id}/elb/ipgroups/{ipgroup_id}                       | elb:ipgroups:delete               | -            |
| GET /v3/{project_id}/elb/ipgroups                                       | elb:ipgroups:list                 | -            |
| GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}                          | elb:ipgroups:show                 | -            |
| PUT /v3/{project_id}/elb/ipgroups/{ipgroup_id}                          | elb:ipgroups:update               | -            |
| POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/create-or-update | elb:ipgroups:update               | -            |
| POST /v3/{project_id}/elb/ipgroups/{ipgroup_id}/iplist/batch-delete     | elb:ipgroups:update               | -            |
| GET /v3/{project_id}/elb/ipgroups/{ipgroup_id}/related-listeners        | elb:ipgroups:showRelatedListeners | -            |
| POST /v3/{project_id}/elb/security-policies                             | elb:security-policies:create      | -            |
| DELETE /v3/{project_id}/elb/security-policies/{security_policy_id}      | elb:security-policies:delete      | -            |
| GET /v3/{project_id}/elb/security-policies                              | elb:security-policies:list        | -            |

| API                                                             | Action                       | Dependencies |
|-----------------------------------------------------------------|------------------------------|--------------|
| GET /v3/{project_id}/elb/system-security-policies               | elb:security-policies:list   | -            |
| GET /v3/{project_id}/elb/security-policies/{security_policy_id} | elb:security-policies:show   | -            |
| PUT /v3/{project_id}/elb/security-policies/{security_policy_id} | elb:security-policies:update | -            |
| POST /v3/{project_id}/elb/pools/{pool_id}/members               | elb:members:create           | -            |
| DELETE /v3/{project_id}/elb/pools/{pool_id}/members/{member_id} | elb:members:delete           | -            |
| GET /v3/{project_id}/elb/pools/{pool_id}/members                | elb:members:list             | -            |
| GET /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}    | elb:members:show             | -            |
| PUT /v3/{project_id}/elb/pools/{pool_id}/members/{member_id}    | elb:members:update           | -            |
| POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-update  | elb:members:update           | -            |
| POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-add     | elb:members:create           | -            |

| API                                                            | Action               | Dependencies |
|----------------------------------------------------------------|----------------------|--------------|
| POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-delete | elb:members:delete   | -            |
| POST /v3/{project_id}/elb/pools                                | elb:pools:create     | -            |
| DELETE /v3/{project_id}/elb/pools/{pool_id}                    | elb:pools:delete     | -            |
| GET /v3/{project_id}/elb/pools                                 | elb:pools:list       | -            |
| GET /v3/{project_id}/elb/pools/{pool_id}                       | elb:pools:show       | -            |
| PUT /v3/{project_id}/elb/pools/{pool_id}                       | elb:pools:update     | -            |
| POST /v3/{project_id}/elb/master-slave-pools                   | elb:pools:create     | -            |
| GET /v3/{project_id}/elb/master-slave-pools                    | elb:pools:list       | -            |
| GET /v3/{project_id}/elb/master-slave-pools/{pool_id}          | elb:pools:show       | -            |
| DELETE /v3/{project_id}/elb/master-slave-pools/{pool_id}       | elb:pools:delete     | -            |
| POST /v3/{project_id}/elb/listeners                            | elb:listeners:create | -            |
| DELETE /v3/{project_id}/elb/listeners/{listener_id}            | elb:listeners:delete | -            |

| API                                                           | Action                      | Dependencies |
|---------------------------------------------------------------|-----------------------------|--------------|
| DELETE /v3/{project_id}/elb/listeners/{listener_id}/force     | elb:listeners:delete        | -            |
| GET /v3/{project_id}/elb/listeners                            | elb:listeners:list          | -            |
| GET /v3/{project_id}/elb/listeners/{listener_id}              | elb:listeners:show          | -            |
| PUT /v3/{project_id}/elb/listeners/{listener_id}              | elb:listeners:update        | -            |
| POST /v3/{project_id}/elb/healthmonitors                      | elb:healthmonitors:create   | -            |
| DELETE /v3/{project_id}/elb/healthmonitors/{healthmonitor_id} | elb:healthmonitors:delete   | -            |
| GET /v3/{project_id}/elb/healthmonitors                       | elb:healthmonitors:list     | -            |
| GET /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}    | elb:healthmonitors:show     | -            |
| PUT /v3/{project_id}/elb/healthmonitors/{healthmonitor_id}    | elb:healthmonitors:update   | -            |
| GET /v3/{project_id}/elb/availability-zones                   | elb:availability-zones:list | -            |
| GET /v3/{project_id}/elb/preoccupy-ip-num                     | elb:loadbalancers:show      | -            |
| POST /v3/{project_id}/elb/logtanks                            | elb:logtanks:create         | -            |



| API                                                              | Action                             | Dependencies |
|------------------------------------------------------------------|------------------------------------|--------------|
| DELETE /v3/{project_id}/elb/logtanks/{logtank_id}                | elb:logtanks:delete                | -            |
| GET /v3/{project_id}/elb/logtanks                                | elb:logtanks:list                  | -            |
| GET /v3/{project_id}/elb/logtanks/{logtank_id}                   | elb:logtanks:show                  | -            |
| PUT /v3/{project_id}/elb/logtanks/{logtank_id}                   | elb:logtanks:update                | -            |
| POST /v3/{project_id}/elb/certificates                           | elb:certificates:create            | -            |
| DELETE /v3/{project_id}/elb/certificates/{certificate_id}        | elb:certificates:delete            | -            |
| GET /v3/{project_id}/elb/certificates                            | elb:certificates:list              | -            |
| GET /v3/{project_id}/elb/certificates/{certificate_id}           | elb:certificates:show              | -            |
| PUT /v3/{project_id}/elb/certificates/{certificate_id}           | elb:certificates:update            | -            |
| POST /v3/{project_id}/elb/certificates/settings/private-key-echo | elb:certificates:setPrivateKeyEcho | -            |
| GET /v3/{project_id}/elb/certificates/settings/private-key-echo  | elb:certificates:getPrivateKeyEcho | -            |

| API                                                                    | Action                | Dependencies |
|------------------------------------------------------------------------|-----------------------|--------------|
| POST /v3/{project_id}/elb/l7policies                                   | elb:l7policies:create | -            |
| DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}                   | elb:l7policies:delete | -            |
| GET /v3/{project_id}/elb/l7policies                                    | elb:l7policies:list   | -            |
| GET /v3/{project_id}/elb/l7policies/{l7policy_id}                      | elb:l7policies:show   | -            |
| PUT /v3/{project_id}/elb/l7policies/{l7policy_id}                      | elb:l7policies:update | -            |
| POST /v3/{project_id}/elb/l7policies/batch-update-priority             | elb:l7policies:update | -            |
| POST /v3/{project_id}/elb/l7policies/{l7policy_id}/rules               | elb:l7rules:create    | -            |
| DELETE /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id} | elb:l7rules:delete    | -            |
| GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules                | elb:l7rules:list      | -            |
| GET /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}    | elb:l7rules:show      | -            |

| API                                                                 | Action             | Dependencies |
|---------------------------------------------------------------------|--------------------|--------------|
| PUT /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id} | elb:l7rules:update | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-70](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for ELB.

**Table 3-70** Resource types supported by ELB

| Resource Type    | URN                                                               |
|------------------|-------------------------------------------------------------------|
| pool             | elb:<region>:<account-id>:pool:<pool-id>                          |
| loadbalancer     | elb:<region>:<account-id>:loadbalancer:<loadbalancer-id>          |
| certificate      | elb:<region>:<account-id>:certificate:<certificate-id>            |
| healthmonitor    | elb:<region>:<account-id>:healthmonitor:<healthmonitor-id>        |
| ipgroup          | elb:<region>:<account-id>:ipgroup:<ipgroup-id>                    |
| securityPolicy   | elb:<region>:<account-id>:securityPolicy:<security-policy-id>     |
| logtank          | elb:<region>:<account-id>:logtank:<logtank-id>                    |
| availabilityZone | elb:<region>:<account-id>:availabilityZone:<availability-zone-id> |
| member           | elb:<region>:<account-id>:member:<pool-id>/<member-id>            |
| l7policy         | elb:<region>:<account-id>:l7policy:<l7policy-id>                  |
| l7rule           | elb:<region>:<account-id>:l7rule:<l7policy-id>/<l7rule-id>        |
| flavor           | elb:<region>:<account-id>:flavor:<flavor-id>                      |

| Resource Type | URN                                              |
|---------------|--------------------------------------------------|
| subnet        | vpc:<region>:<account-id>:subnet:<subnet-id>     |
| listener      | elb:<region>:<account-id>:listener:<listener-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, elb) apply only to operations of the xx service. For details, see [Table 3-71](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by ELB

The following table lists the condition keys that you can define in identity policies for ELB. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-71** Service-specific condition keys supported by ELB

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                                                                                                                                                                                                            |
|--------------------------------|---------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| elb:AssociatePublicips         | boolean | Single-valued                 | Filters access based on whether creating or binding a public network is involved during load balancer creation or modification. To prevent the Elastic Load Balancer from accessing the public network, you need to use the EIP-related actions for policy management. |
| elb:UpdateListenerIpgroup      | boolean | Single-valued                 | Filters access permissions based on whether the access control needs to be updated when the listener is modified.                                                                                                                                                      |
| elb:OnlyUpdateListenerIpgroup  | boolean | Single-valued                 | Filters access permissions based on whether only the access control needs to be updated when the listener is modified.                                                                                                                                                 |

## 3.4 Containers

### 3.4.1 Cloud Container Engine

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are

available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CCE, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CCE, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CCE.

**Table 3-72** Actions supported by CCE

| Action                       | Description                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                |
|------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------|
| cce:imageCache:create        | Grants permission to create image cache.                          | Write        | -                           | -             | -                                                                    |
| cce:imageCache:delete        | Grants permission to delete image cache.                          | Write        | imageCache *                | -             | -                                                                    |
| cce:imageCache:list          | Grants permission to return the list of all image caches.         | List         | -                           | -             | -                                                                    |
| cce:imageCache:get           | Grants permission to return details of the specified image cache. | Read         | imageCache *                | -             | -                                                                    |
| cce:packageProduct:list      | Grants permission to return the list of all package products.     | List         | -                           | -             | -                                                                    |
| cce:packageProduct:subscribe | Grants permission to subscribe package products.                  | Write        | -                           | -             | -                                                                    |
| cce:cluster:createCluster    | Grants permission to create cluster.                              | Write        | cluster *                   | -             | <ul style="list-style-type: none"> <li>cce:cluster:create</li> </ul> |

| Action                    | Description                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                        | Alias                |
|---------------------------|---------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
|                           |                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">cce:AssociatePublicIp</a></li> <li>• <a href="#">cce:VpcId</a></li> <li>• <a href="#">cce:SubnetId</a></li> </ul> |                      |
| cce:cluster:delete        | Grants permission to delete cluster.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                   | -                    |
| cce:cluster:updateCluster | Grants permission to update cluster.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                   | • cce:cluster:update |
| cce:cluster:upgrade       | Grants permission to upgrade cluster. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                   | -                    |
| cce:cluster:start         | Grants permission to start cluster.   | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                   | -                    |



| Action                    | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias              |
|---------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| cce:cluster:stop          | Grants permission to stop cluster.                                                            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                  |
| cce:cluster:list          | Grants permission to return the list of all clusters.                                         | List         | cluster *                   | -                                                                                                                                                  | -                  |
| cce:cluster:get Cluster   | Grants permission to return details of the specified cluster.                                 | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cce:cluster: get |
| cce:cluster:get Endpoints | Grants permission to return endpoints of the specified cluster.                               | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cce:cluster: get |
| cce:cluster:resize        | Grants permission to resize cluster.                                                          | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                  |
| cce:cluster:toperiod      | Grants permission to change the billing mode of a cluster from pay-per-use to yearly/monthly. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                  |

| Action                               | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                  |
|--------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| cce:cluster:eip Binding              | Grants permission to bind/unbind eip to cluster.                  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• cce:cluster:update</li> </ul> |
| cce:cluster:generateClientCredential | Grants permission to generate client credential to visit cluster. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• cce:cluster:get</li> </ul>    |
| cce:cluster:revokeClientCredential   | Grants permission to revoke cluster client certificate.           | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                                                                      |
| cce:cluster:rotateCredentials        | Grants permission to rotate cluster credentials.                  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                                                                      |
| cce:cluster:addTags                  | Grants permission to add tags to cluster.                         | Tagging      | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• cce:tag:operate</li> </ul>    |
|                                      |                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul>              |                                                                        |

| Action                               | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                |
|--------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| cce:cluster:removeTags               | Grants permission to remove tags from cluster.              | Tagging      | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | • cce:tag:operate    |
|                                      |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul>                                                  |                      |
| cce:cluster:listTags                 | Grants permission to list tags from clusters.               | Read         | -                           | -                                                                                                                                                                                      | • cce:tag:list       |
| cce:cluster:listTagsForCluster       | Grants permission to list cluster tags.                     | Read         | cluster *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | • cce:cluster:get    |
| cce:cluster:listClustersByTag        | Grants permission to list clusters by tags.                 | Read         | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                              | • cce:cluster:list   |
| cce:cluster:validate                 | Grants permission to check if cluster parameters are valid. | Read         | cluster *                   | -                                                                                                                                                                                      | • cce:cluster:create |
|                                      |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> |                      |
| cce:cluster:getConfigurationTemplate | Grants permission to query cluster configuration template.  | Read         | cluster *                   | -                                                                                                                                                                                      | • cce:cluster:get    |
|                                      |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">cce:ClusterId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                     |                      |

| Action                          | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                                                                |
|---------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| cce:cluster:get Configuration   | Grants permission to get cluster configuration.                       | Read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>cce:cluster:get</li> </ul>    |
| cce:cluster:updateConfiguration | Grants permission to update cluster configuration.                    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>cce:cluster:update</li> </ul> |
| cce:cluster:get LogConfig       | Grants permission to get cluster log config.                          | Read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                                                    |
| cce:cluster:updateLogConfig     | Grants permission to update cluster log config.                       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                                                    |
| cce:cluster:checkLock           | Grants permission to check and release CBC related lock for clusters. | Write        | -                           | -                                                                                                              | -                                                                    |
| cce:partition:create            | Grants permission to generate partition.                              | Write        | cluster *                   | -                                                                                                              | -                                                                    |
|                                 |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul>                 |                                                                      |

| Action               | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                               | Alias |
|----------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cce:partition:update | Grants permission to update partition.                           | Write        | cluster *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                       | -     |
| cce:partition:get    | Grants permission to return details of the specified partition.  | Read         | cluster *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                       | -     |
| cce:partition:list   | Grants permission to return the list of partitions of a cluster. | List         | cluster *                   | -                                                                                                                                                                                                                                                                                           | -     |
|                      |                                                                  |              | -                           | <ul style="list-style-type: none"> <li><a href="#">cce:ClusterId</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                              |       |
| cce:nodepool:create  | Grants permission to create nodepool.                            | Write        | cluster *                   | -                                                                                                                                                                                                                                                                                           | -     |
|                      |                                                                  |              | -                           | <ul style="list-style-type: none"> <li><a href="#">cce:ClusterId</a></li> <li><a href="#">evs:Encrypted</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">cce:Subnets</a></li> <li><a href="#">cce:KmsKeys</a></li> <li><a href="#">cce:AvailableZones</a></li> </ul> |       |
| cce:nodepool:delete  | Grants permission to delete nodepool.                            | Write        | cluster *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                       | -     |

| Action                       | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                        | Alias                                                                 |
|------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| cce:nodepool:updateNodepool  | Grants permission to update nodepool.                           | Write        | cluster *                   | -                                                                                                                                                                    | <ul style="list-style-type: none"> <li>cce:nodepool:update</li> </ul> |
|                              |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>evs:Encrypted</li> <li>g:EnterpriseProjectId</li> <li>cce:Subnets</li> <li>cce:KmsKeys</li> <li>cce:AvailableZones</li> </ul> |                                                                       |
| cce:nodepool:upgradeNodepool | Grants permission to upgrade nodepool.                          | Write        | cluster *                   | -                                                                                                                                                                    | <ul style="list-style-type: none"> <li>cce:nodepool:update</li> </ul> |
|                              |                                                                 |              | -                           | g:EnterpriseProjectId                                                                                                                                                |                                                                       |
| cce:nodepool:scale           | Grants permission to scale nodepool.                            | Write        | cluster *                   | g:EnterpriseProjectId                                                                                                                                                | -                                                                     |
| cce:nodepool:getNodepool     | Grants permission to return details of the specified nodepool.  | Read         | cluster *                   | g:EnterpriseProjectId                                                                                                                                                | <ul style="list-style-type: none"> <li>cce:nodepool:get</li> </ul>    |
| cce:nodepool:list            | Grants permission to return the list of nodepools of a cluster. | List         | cluster *                   | -                                                                                                                                                                    | -                                                                     |
|                              |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul>                                                                       |                                                                       |
| cce:nodepool:getQuota        | Grants permission to get nodepool quotas.                       | Read         | cluster *                   | -                                                                                                                                                                    | <ul style="list-style-type: none"> <li>cce:nodepool:get</li> </ul>    |

| Action                                | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                  | Alias                 |
|---------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------|-----------------------|
|                                       |                                                                |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> |                       |
| cce:nodepool:migrate                  | Grants permission to migrate nodes between node pools.         | Write        | cluster *                   | -                                                                                              | • cce:nodepool:update |
|                                       |                                                                |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> |                       |
| cce:nodepool:sync                     | Grants permission to sync configuration to nodes in node pool. | Write        | cluster *                   | g:EnterpriseProjectId                                                                          | • cce:nodepool:get    |
| cce:nodepool:getConfigurationTemplate | Grants permission to get configuration template of node pool.  | Read         | cluster *                   | g:EnterpriseProjectId                                                                          | • cce:nodepool:get    |
| cce:nodepool:getConfiguration         | Grants permission to get configuration of node pool.           | Read         | cluster *                   | g:EnterpriseProjectId                                                                          | • cce:nodepool:get    |
| cce:nodepool:updateConfiguration      | Grants permission to update configuration of node pool.        | Write        | cluster *                   | g:EnterpriseProjectId                                                                          | • cce:nodepool:update |
| cce:node:createNode                   | Grants permission to create node.                              | Write        | cluster *                   | -                                                                                              | • cce:node:create     |

| Action                | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                            | Alias          |
|-----------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                       |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">cce:ClusterId</a></li> <li>• <a href="#">evs:Encrypted</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">cce:AssociatePublicIp</a></li> <li>• <a href="#">cce:Subnets</a></li> <li>• <a href="#">cce:KmsKeys</a></li> <li>• <a href="#">cce:AvailableZones</a></li> </ul> |                |
| cce:node:reportStatus | Grants permission to report node status.                    | Write        | cluster *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                    | • cce:node:get |
| cce:node:delete       | Grants permission to delete node.                           | Write        | cluster *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                    | -              |
| cce:node:update       | Grants permission to update node.                           | Write        | cluster *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                    | -              |
| cce:node:getNode      | Grants permission to return details of the specified node.  | Read         | cluster *                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                    | • cce:node:get |
| cce:node:list         | Grants permission to return the list of nodes of a cluster. | List         | cluster *                   | -                                                                                                                                                                                                                                                                                                                                                        | -              |
|                       |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">cce:ClusterId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                                                                       |                |



| Action           | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                              | Alias                                                             |
|------------------|-----------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| cce:node:reset   | Grants permission to reset nodes.                   | Write        | cluster *                   | -                                                                                                                                          | <ul style="list-style-type: none"> <li>cce:node:create</li> </ul> |
|                  |                                                     |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>evs:Encrypted</li> <li>g:EnterpriseProjectId</li> <li>cce:KmsKeys</li> </ul> |                                                                   |
| cce:node:add     | Grants permission to add nodes.                     | Write        | cluster *                   | -                                                                                                                                          | <ul style="list-style-type: none"> <li>cce:node:create</li> </ul> |
|                  |                                                     |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>evs:Encrypted</li> <li>g:EnterpriseProjectId</li> <li>cce:KmsKeys</li> </ul> |                                                                   |
| cce:node:remove  | Grants permission to remove nodes.                  | Write        | cluster *                   | -                                                                                                                                          | -                                                                 |
|                  |                                                     |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul>                                             |                                                                   |
| cce:node:migrate | Grants permission to migrate node between clusters. | Write        | cluster *                   | -                                                                                                                                          | -                                                                 |

| Action            | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                         | Alias                                                             |
|-------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
|                   |                                                                                       |              | -                           | <ul style="list-style-type: none"> <li>cce:nodeTransferSourceCluster</li> <li>cce:nodeTransferTargetCluster</li> <li>g:EnterpriseProjectId</li> </ul> |                                                                   |
| cce:node:unlock   | Grants permission to unlock nodes.                                                    | Write        | cluster *                   | -                                                                                                                                                     | <ul style="list-style-type: none"> <li>cce:node:update</li> </ul> |
|                   |                                                                                       |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul>                                                        |                                                                   |
| cce:node:sync     | Grants permission to sync IaaS status of node.                                        | Read         | cluster *                   | g:EnterpriseProjectId                                                                                                                                 | <ul style="list-style-type: none"> <li>cce:node:get</li> </ul>    |
| cce:node:toperiod | Grants permission to change billing mode of nodes from pay-per-use to yearly/monthly. | Write        | cluster *                   | -                                                                                                                                                     | -                                                                 |
|                   |                                                                                       |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul>                                                        |                                                                   |
| cce:job:delete    | Grants permission to delete job.                                                      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul>                                                        | -                                                                 |
| cce:job:get       | Grants permission to return details of a job.                                         | Read         | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul>                                                        | -                                                                 |

| Action                   | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                  | Alias |
|--------------------------|------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------|-------|
| cce:job:list             | Grants permission to return the list of jobs.              | List         | cluster *                   | -                                                                                              | -     |
|                          |                                                            |              | -                           | cce:ClusterId                                                                                  |       |
| cce:quota:get            | Grants permission to query the cce related resource quota. | Read         | -                           | -                                                                                              | -     |
| cce:addonInstance:create | Grants permission to create addon instance.                | Write        | cluster *                   | -                                                                                              | -     |
|                          |                                                            |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> |       |
| cce:addonInstance:delete | Grants permission to delete addon instance.                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| cce:addonInstance:update | Grants permission to update addon instance.                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| cce:addonInstance:get    | Grants permission to return details of addon instance.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> | -     |
| cce:addonInstance:list   | Grants permission to return the list of addon instances.   | List         | cluster *                   | -                                                                                              | -     |

| Action                     | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                      | Alias                                                              |
|----------------------------|-------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
|                            |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">cce:ClusterId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                    |
| cce:addonInstance:rollback | Grants permission to return rollback of addon instance.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">cce:ClusterId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                  |
| cce:chart:upload           | Grants permission to upload charts.                         | Write        | -                           | -                                                                                                                                  | -                                                                  |
| cce:chart:delete           | Grants permission to delete charts.                         | Write        | -                           | -                                                                                                                                  | -                                                                  |
| cce:chart:update           | Grants permission to update charts.                         | Write        | -                           | -                                                                                                                                  | -                                                                  |
| cce:chart:listChart        | Grants permission to return the list of all charts.         | List         | -                           | -                                                                                                                                  | <ul style="list-style-type: none"> <li>• cce:chart:list</li> </ul> |
| cce:chart:getChart         | Grants permission to return details of the specified chart. | Read         | -                           | -                                                                                                                                  | <ul style="list-style-type: none"> <li>• cce:chart:get</li> </ul>  |
| cce:chart:download         | Grants permission to download chart.                        | Read         | -                           | -                                                                                                                                  | <ul style="list-style-type: none"> <li>• cce:chart:get</li> </ul>  |
| cce:chart:getQuota         | Grants permission to get quota of chart.                    | Read         | -                           | -                                                                                                                                  | <ul style="list-style-type: none"> <li>• cce:chart:list</li> </ul> |

| Action                          | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                  | Alias                                                                 |
|---------------------------------|-----------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| cce:release:create              | Grants permission to create release.                | Write        | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> | -                                                                     |
| cce:release:delete              | Grants permission to delete release.                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> | -                                                                     |
| cce:release:update              | Grants permission to update release.                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> | -                                                                     |
| cce:release:get                 | Grants permission to query details of release.      | Read         | cluster *                   | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> | -                                                                     |
| cce:release:list                | Grants permission to query the list of releases.    | List         | cluster *                   | -                                                                                              | -                                                                     |
|                                 |                                                     |              | -                           | <ul style="list-style-type: none"> <li>cce:ClusterId</li> <li>g:EnterpriseProjectId</li> </ul> |                                                                       |
| cce:permissionApplyOrder:create | Grants permission to create permission apply order. | Write        | -                           | -                                                                                              | <ul style="list-style-type: none"> <li>cce:cluster:upgrade</li> </ul> |
| cce:permissionApplyOrder:list   | Grants permission to list permission apply orders.  | List         | -                           | -                                                                                              | <ul style="list-style-type: none"> <li>cce:cluster:list</li> </ul>    |

| Action                           | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cce:longaksk:getConfig           | Grants permission to get longAKSK config.            | Read         | -                           | -                                                                                                                                                  | -     |
| cce:longaksk:updateConfig        | Grants permission to update longAKSK config.         | Write        | -                           | -                                                                                                                                                  | -     |
| cce:cluster:getLongAKSKConfig    | Grants permission to get cluster longAKSK config.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| cce:cluster:updateLongAKSKConfig | Grants permission to update cluster longAKSK config. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| cce:accessPolicy:get             | Grants permission to get access policy.              | Read         | -                           | -                                                                                                                                                  | -     |
| cce:accessPolicy:list            | Grants permission to list access policy.             | Read         | -                           | -                                                                                                                                                  | -     |
| cce:accessPolicy:post            | Grants permission to create access policy.           | Write        | -                           | -                                                                                                                                                  | -     |
| cce:accessPolicy:put             | Grants permission to update access policy.           | Write        | -                           | -                                                                                                                                                  | -     |

| Action                       | Description                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| cce:accessPolicy:delete      | Grants permission to delete access policy.                     | Write        | -                           | -             | -     |
| cce:imageCache:get           | Grants permission to get image cache.                          | Read         | -                           | -             | -     |
| cce:imageCache:list          | Grants permission to list image caches.                        | List         | -                           | -             | -     |
| cce:imageCache:create        | Grants permission to create image cache.                       | Write        | -                           | -             | -     |
| cce:imageCache:delete        | Grants permission to delete image cache.                       | Write        | -                           | -             | -     |
| cce:hypernode:list           | Grants permission to return the list of hypernodes in cluster. | List         | cluster *                   | -             | -     |
| cce:packageProduct:list      | Grants permission to return the list of all package products.  | List         | -                           | -             | -     |
| cce:packageProduct:subscribe | Grants permission to subscribe package products.               | Write        | -                           | -             | -     |

Each API of CCE usually supports one or more actions. [Table 3-73](#) lists the supported actions and dependencies.

**Table 3-73** Actions and dependencies supported by CCE APIs

| API                                                                                         | Action                               | Dependencies |
|---------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| POST /v5/<br>imagecaches                                                                    | cce:imageCache:create                | -            |
| DELETE /v5/<br>imagecaches/<br>{image_cache_id}                                             | cce:imageCache:delete                | -            |
| GET /v5/<br>imagecaches/<br>{image_cache_id}                                                | cce:imageCache:get                   | -            |
| GET /v5/<br>imagecaches                                                                     | cce:imageCache:list                  | -            |
| GET /v5/package-<br>products                                                                | cce:packageProduct:list              | -            |
| POST /v5/package-<br>products/subscribe                                                     | cce:packageProduct:subscri<br>be     | -            |
| GET /api/v3/<br>projects/<br>{project_id}/<br>longaksk/config                               | cce:longaksk:getConfig               | -            |
| PUT /api/v3/<br>projects/<br>{project_id}/<br>longaksk/config                               | cce:longaksk:updateConfig            | -            |
| GET /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>longaksk/config | cce:cluster:getLongAKSKCo<br>nfig    | -            |
| PUT /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>longaksk/config | cce:cluster:updateLongAKS<br>KConfig | -            |
| GET /api/v3/access-<br>policies/{policy_id}                                                 | cce:accessPolicy:get                 | -            |
| GET /api/v3/access-<br>policies                                                             | cce:accessPolicy:list                | -            |
| POST /api/v3/<br>access-policies                                                            | cce:accessPolicy:post                | -            |



| API                                                                                       | Action                    | Dependencies |
|-------------------------------------------------------------------------------------------|---------------------------|--------------|
| PUT /api/v3/access-policies/{policy_id}                                                   | cce:accessPolicy:put      | -            |
| DELETE /api/v3/access-policies/{policy_id}                                                | cce:accessPolicy:delete   | -            |
| GET /api/v3/projects/{project_id}/quotas                                                  | cce:quota:get             | -            |
| POST /api/v3/projects/{project_id}/clusters                                               | cce:cluster:createCluster | -            |
| DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}                                | cce:cluster:delete        | -            |
| PUT /api/v3/projects/{project_id}/clusters/{cluster_id}                                   | cce:cluster:updateCluster | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade                | cce:cluster:upgrade       | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/retry          | cce:cluster:upgrade       | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks/{task_id} | cce:cluster:getCluster    | -            |

| API                                                                                                                                        | Action                 | Dependencies |
|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--------------|
| POST /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>operation/upgrade/<br>continue                                | cce:cluster:upgrade    | -            |
| GET /api/v3.1/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>operation/snapshot/<br>tasks                                 | cce:cluster:getCluster | -            |
| POST /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>operation/<br>upgradeworkflows                                | cce:cluster:upgrade    | -            |
| GET /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>operation/<br>upgradeworkflows                                 | cce:cluster:getCluster | -            |
| GET /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>operation/upgrade/<br>tasks                                    | cce:cluster:getCluster | -            |
| PATCH /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>operation/<br>upgradeworkflows/<br>{upgrade_workflow<br>_id} | cce:cluster:upgrade    | -            |

| API                                                                                                      | Action                   | Dependencies |
|----------------------------------------------------------------------------------------------------------|--------------------------|--------------|
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id} | cce:cluster:getCluster   | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/pause                         | cce:cluster:upgrade      | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/awake                                 | cce:cluster:start        | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/hibernate                             | cce:cluster:stop         | -            |
| GET /api/v3/projects/{project_id}/clusters                                                               | cce:cluster:list         | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}                                                  | cce:cluster:getCluster   | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/openapi                                          | cce:cluster:getEndpoints | -            |
| GET /v5/imagecaches/{image_cache_id}                                                                     | cce:imageCache:get       | -            |
| GET /v5/imagecaches                                                                                      | cce:imageCache:list      | -            |

| API                                                                                            | Action                                   | Dependencies |
|------------------------------------------------------------------------------------------------|------------------------------------------|--------------|
| POST /v5/<br>imagecaches                                                                       | cce:imageCache:create                    | -            |
| DELETE /v5/<br>imagecaches/<br>{image_cache_id}                                                | cce:imageCache:delete                    | -            |
| GET /v5/package-<br>products                                                                   | cce:packageProduct:list                  | -            |
| POST /v5/package-<br>products/subscribe                                                        | cce:packageProduct:subscri<br>be         | -            |
| POST /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>operation/resize  | cce:cluster:resize                       | -            |
| PUT /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>mastereip          | cce:cluster:eipBinding                   | -            |
| POST /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>clustercert       | cce:cluster:generateClientCr<br>edential | -            |
| POST /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>clustercertrevoke | cce:cluster:revokeClientCre-<br>dential  | -            |
| POST /api/v3/<br>projects/<br>{project_id}/<br>clusters/<br>{cluster_id}/tags/<br>create       | cce:cluster:addTags                      | -            |

| API                                                                                 | Action                 | Dependencies |
|-------------------------------------------------------------------------------------|------------------------|--------------|
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/tags/delete                | cce:cluster:removeTags | -            |
| PUT /v1/services/checklock/cce                                                      | cce:cluster:checkLock  | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions                 | cce:partition:create   | -            |
| PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions/{partition_name} | cce:partition:update   | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions/{partition_name} | cce:partition:get      | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions                  | cce:partition:list     | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools                  | cce:nodepool:create    | -            |

| API                                                                                                | Action                       | Dependencies |
|----------------------------------------------------------------------------------------------------|------------------------------|--------------|
| DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}                 | cce:nodepool:delete          | -            |
| PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}                    | cce:nodepool:updateNodepool  | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/operation/upgrade | cce:nodepool:upgradeNodepool | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/operation/scale   | cce:nodepool:scale           | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}                    | cce:nodepool:getNodepool     | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools                                  | cce:nodepool:list            | -            |

| API                                                                                                  | Action                                | Dependencies |
|------------------------------------------------------------------------------------------------------|---------------------------------------|--------------|
| PUT /api/v3.1/projects/{project_id}/clusters/{cluster_id}/nodepool/{nodepool_id}/sync                | cce:nodepool:sync                     | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration/detail | cce:nodepool:getConfigurationTemplate | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes                                       | cce:node:createNode                   | -            |
| DELETE /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}                           | cce:node:delete                       | -            |
| PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}                              | cce:node:update                       | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}                              | cce:node:getNode                      | -            |
| GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes                                        | cce:node:list                         | -            |

| API                                                                                                   | Action           | Dependencies |
|-------------------------------------------------------------------------------------------------------|------------------|--------------|
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/sync                                   | cce:node:update  | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/nodes/add            | cce:node:add     | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/reset                                  | cce:node:reset   | -            |
| POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/add                                    | cce:node:add     | -            |
| PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/operation/remove                        | cce:node:remove  | -            |
| PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes/operation/migrateto/{target_cluster_id} | cce:node:migrate | -            |
| GET /api/v2/projects/{project_id}/clusters/{cluster_id}/nodes/{node_id}/sync                          | cce:node:sync    | -            |



| API                                                | Action                     | Dependencies |
|----------------------------------------------------|----------------------------|--------------|
| DELETE /api/v2/projects/{project_id}/jobs/{job_id} | cce:job:delete             | -            |
| GET /api/v3/projects/{project_id}/jobs/{job_id}    | cce:job:get                | -            |
| GET /api/v2/projects/{project_id}/jobs             | cce:job:list               | -            |
| GET /api/v3/addontemplates                         | cce:cluster:list           | -            |
| POST /api/v3/addons                                | cce:addonInstance:create   | -            |
| DELETE /api/v3/addons/{id}                         | cce:addonInstance:delete   | -            |
| PUT /api/v3/addons/{id}                            | cce:addonInstance:update   | -            |
| GET /api/v3/addons/{id}                            | cce:addonInstance:get      | -            |
| GET /api/v3/addons                                 | cce:addonInstance:list     | -            |
| POST /api/v3/addons/{id}/operation/rollback        | cce:addonInstance:rollback | -            |
| POST /v2/charts                                    | cce:chart:upload           | -            |
| DELETE /v2/charts/{chart_id}                       | cce:chart:delete           | -            |
| PUT /v2/charts/{chart_id}                          | cce:chart:update           | -            |
| GET /v2/charts/{chart_id}                          | cce:chart:getChart         | -            |
| GET /v2/charts                                     | cce:chart:listChart        | -            |
| GET /v2/charts/{chart_id}/archive                  | cce:chart:download         | -            |
| POST /cce/cam/v3/clusters/{cluster_id}/releases    | cce:release:create         | -            |

| API                                                                            | Action                               | Dependencies |
|--------------------------------------------------------------------------------|--------------------------------------|--------------|
| DELETE /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name} | cce:release:delete                   | -            |
| PUT /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}    | cce:release:update                   | -            |
| GET /cce/cam/v3/clusters/{cluster_id}/namespace/{namespace}/releases/{name}    | cce:release:get                      | -            |
| GET /cce/cam/v3/clusters/{cluster_id}/releases                                 | cce:release:list                     | -            |
| POST /autopilot/v3/projects/{project_id}/clusters                              | cce:cluster:createCluster            | -            |
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/clustercert     | cce:cluster:generateClientCredential | -            |
| DELETE /autopilot/v3/projects/{project_id}/clusters/{cluster_id}               | cce:cluster:delete                   | -            |
| GET /autopilot/v3/projects/{project_id}/clusters                               | cce:cluster:list                     | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}                  | cce:cluster:getCluster               | -            |

| API                                                                              | Action                     | Dependencies |
|----------------------------------------------------------------------------------|----------------------------|--------------|
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/openapi            | cce:cluster:getEndpoints   | -            |
| GET /autopilot/v3/projects/{project_id}/jobs/{job_id}                            | cce:job:get                | -            |
| PUT /autopilot/v3/projects/{project_id}/clusters/{cluster_id}                    | cce:cluster:updateCluster  | -            |
| PUT /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/mastereip          | cce:cluster:eipBinding     | -            |
| POST /autopilot/v3/addons                                                        | cce:addonInstance:create   | -            |
| DELETE /autopilot/v3/addons/{id}                                                 | cce:addonInstance:delete   | -            |
| PUT /autopilot/v3/addons/{id}                                                    | cce:addonInstance:update   | -            |
| GET /autopilot/v3/addons/{id}                                                    | cce:addonInstance:get      | -            |
| GET /autopilot/v3/addons                                                         | cce:addonInstance:list     | -            |
| POST /autopilot/v3/addons/{id}/operation/rollback                                | cce:addonInstance:rollback | -            |
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade | cce:cluster:upgrade        | -            |

| API                                                                                              | Action                 | Dependencies |
|--------------------------------------------------------------------------------------------------|------------------------|--------------|
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/retry           | cce:cluster:upgrade    | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks/{task_id}  | cce:cluster:getCluster | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks/{task_id} | cce:cluster:getCluster | -            |
| GET /autopilot/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot/tasks         | cce:cluster:getCluster | -            |
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows        | cce:cluster:upgrade    | -            |
| POST /autopilot/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot              | cce:cluster:upgrade    | -            |

| API                                                                                                              | Action                 | Dependencies |
|------------------------------------------------------------------------------------------------------------------|------------------------|--------------|
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows                         | cce:cluster:getCluster | -            |
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck                                | cce:cluster:upgrade    | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks                           | cce:cluster:getCluster | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/upgradeinfo                                        | cce:cluster:getCluster | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks                            | cce:cluster:getCluster | -            |
| PATCH /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id} | cce:cluster:upgrade    | -            |

| API                                                                                                            | Action                 | Dependencies |
|----------------------------------------------------------------------------------------------------------------|------------------------|--------------|
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/postcheck                             | cce:cluster:upgrade    | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id} | cce:cluster:getCluster | -            |
| GET /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/upgradeplans                                     | cce:cluster:getCluster | -            |
| PUT /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/upgradeplans/{upgrade_plan_id}                   | cce:cluster:upgrade    | -            |
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/tags/create                                     | cce:cluster:addTags    | -            |
| POST /autopilot/v3/projects/{project_id}/clusters/{cluster_id}/tags/delete                                     | cce:cluster:removeTags | -            |
| GET /autopilot/v3/projects/{project_id}/quotas                                                                 | cce:quota:get          | -            |
| POST /autopilot/v2/charts                                                                                      | cce:chart:upload       | -            |

| API                                                                                                          | Action              | Dependencies |
|--------------------------------------------------------------------------------------------------------------|---------------------|--------------|
| DELETE /<br>autopilot/v2/charts/<br>{chart_id}                                                               | cce:chart:delete    | -            |
| PUT /autopilot/v2/<br>charts/{chart_id}                                                                      | cce:chart:update    | -            |
| GET /autopilot/v2/<br>charts/{chart_id}                                                                      | cce:chart:getChart  | -            |
| GET /autopilot/v2/<br>charts                                                                                 | cce:chart:listChart | -            |
| GET /autopilot/v2/<br>charts/{chart_id}/<br>archive                                                          | cce:chart:download  | -            |
| GET /autopilot/v2/<br>charts/{project_id}/<br>quotas                                                         | cce:chart:getQuota  | -            |
| GET /autopilot/v2/<br>charts/{chart_id}/<br>values                                                           | cce:chart:getChart  | -            |
| POST /<br>autopilot/cam/v3/<br>clusters/<br>{cluster_id}/releases                                            | cce:release:create  | -            |
| DELETE /<br>autopilot/cam/v3/<br>clusters/<br>{cluster_id}/<br>namespace/<br>{namespace}/<br>releases/{name} | cce:release:delete  | -            |
| PUT /<br>autopilot/cam/v3/<br>clusters/<br>{cluster_id}/<br>namespace/<br>{namespace}/<br>releases/{name}    | cce:release:update  | -            |
| GET /<br>autopilot/cam/v3/<br>clusters/<br>{cluster_id}/<br>namespace/<br>{namespace}/<br>releases/{name}    | cce:release:get     | -            |

| API                                                                                                                   | Action           | Dependencies |
|-----------------------------------------------------------------------------------------------------------------------|------------------|--------------|
| GET /<br>autopilot/cam/v3/<br>clusters/<br>{cluster_id}/releases                                                      | cce:release:list | -            |
| GET /<br>autopilot/cam/v3/<br>clusters/<br>{cluster_id}/<br>namespace/<br>{namespace}/<br>releases/{name}/<br>history | cce:release:get  | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-74](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CCE.

**Table 3-74** Resource types supported by CCE

| Resource Type  | URN                                                            |
|----------------|----------------------------------------------------------------|
| cluster        | cce:<region>:<account-id>:cluster:<cluster-name>               |
| imageCache     | cce:<region>:<account-id>:imageCache:<imageCache-name>         |
| packageProduct | cce:<region>:<account-id>:packageProduct:<packageProduct-name> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the



system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).

- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, cce) apply only to operations of the xx service. For details, see [Table 3-75](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

#### Service-specific condition keys supported by CCE

The following table lists the condition keys that you can define in identity policies for CCE. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-75** Service-specific condition keys supported by CCE

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                           |
|--------------------------------|---------|-------------------------------|-----------------------------------------------------------------------|
| cce:ClusterId                  | string  | Single-valued                 | Filters access by the cluster ID that is passed in the request.       |
| cce:nodeTransferSourceCluster  | string  | Single-valued                 | Filters access by the cluster ID from whom nodes migrate.             |
| cce:nodeTransferTargetCluster  | string  | Single-valued                 | Filters access by the cluster ID to whom nodes migrate.               |
| cce:AssociatePublicIp          | boolean | Single-valued                 | Filters access by the associate switch value for binding eip to node. |
| cce:VpcId                      | string  | Single-valued                 | Filters access by the vpc id.                                         |
| cce:SubnetId                   | string  | Single-valued                 | Filters access by the subnet id.                                      |

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                           |
|--------------------------------|--------|-------------------------------|---------------------------------------|
| cce:Subnets                    | string | Multivalued                   | Filters access by the subnet ids.     |
| cce:KmsKeys                    | string | Multivalued                   | Filters access by the kms key ids.    |
| cce:AvailableZones             | string | Multivalued                   | Filters access by the availableZones. |

## 3.4.2 Cloud Container Instance

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an SCP.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an SCP.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions, and you must specify all resources ("\*") in your SCP statements.

- If this column includes a resource type, you must specify the URN in the Resource element of your statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CCI, see [Resources](#).

- The **Condition Key** column includes keys that you can specify in the Condition element of an SCP statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CCI, see [Conditions](#).

The following table lists the actions that you can define in statements for CCI.

**Table 3-76** Actions supported by CCI

| Action               | Description                               | Access Level | Resource Type (*: required) | Condition Key                                 |
|----------------------|-------------------------------------------|--------------|-----------------------------|-----------------------------------------------|
| cci:namespace:list   | Grants permission to list all namespaces. | List         | Namespace *                 | -                                             |
| cci:namespace:create | Grants permission to create a namespace.  | Write        | Namespace *                 | -                                             |
| cci:namespace:get    | Grants permission to query a namespace.   | Read         | Namespace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |
| cci:namespace:delete | Grants permission to delete a namespace.  | Write        | Namespace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |
| cci:network:list     | Grants permission to list all secrets.    | List         | Network *                   | -                                             |
| cci:network:create   | Grants permission to create a network.    | Write        | Network *                   | -                                             |
| cci:network:get      | Grants permission to query a network.     | Read         | Network *                   | -                                             |

| Action               | Description                                 | Access Level | Resource Type (*: required) | Condition Key                         |
|----------------------|---------------------------------------------|--------------|-----------------------------|---------------------------------------|
| cci:network:delete   | Grants permission to delete a network.      | Write        | Network *                   | -                                     |
| cci:network:update   | Grants permission to update a network.      | Write        | Network *                   | -                                     |
| cci:configmap:list   | Grants permission to list all ConfigMaps.   | List         | ConfigMap *                 | -                                     |
| cci:configmap:create | Grants permission to create a ConfigMap.    | Write        | ConfigMap *                 | -                                     |
| cci:configmap:get    | Grants permission to query a ConfigMap.     | Read         | ConfigMap *                 | -                                     |
| cci:configmap:delete | Grants permission to delete a ConfigMap.    | Write        | ConfigMap *                 | -                                     |
| cci:configmap:update | Grants permission to update a ConfigMap.    | Write        | ConfigMap *                 | -                                     |
| cci:pod:list         | Grants permission to list all pods.         | List         | Pod *                       | -                                     |
| cci:pod:create       | Grants permission to create a pod.          | Write        | Pod *                       | <a href="#">cci:AssociatePublicIp</a> |
| cci:pod:get          | Grants permission to query a pod.           | Read         | Pod *                       | -                                     |
| cci:pod:delete       | Grants permission to delete a pod.          | Write        | Pod *                       | -                                     |
| cci:pod:update       | Grants permission to update a pod.          | Write        | Pod *                       | -                                     |
| cci:pod:getLog       | Grants permission to query pod logs.        | Read         | Pod *                       | -                                     |
| cci:pod:exec         | Grants permission to run commands in a pod. | Write        | Pod *                       | <a href="#">cci:ContainerName</a>     |

| Action                           | Description                                           | Access Level | Resource Type (*: required) | Condition Key |
|----------------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|
| cci:secret:list                  | Grants permission to list all secrets.                | List         | Secret *                    | -             |
| cci:secret:create                | Grants permission to create a secret.                 | Write        | Secret *                    | -             |
| cci:secret:get                   | Grants permission to query a secret.                  | Read         | Secret *                    | -             |
| cci:secret:delete                | Grants permission to delete a secret.                 | Write        | Secret *                    | -             |
| cci:secret:update                | Grants permission to update a secret.                 | Write        | Secret *                    | -             |
| cci:persistentvolume:list        | Grants permission to list all PersistentVolumes.      | List         | PersistentVolume *          | -             |
| cci:persistentvolume:create      | Grants permission to create a PersistentVolume.       | Write        | PersistentVolume *          | -             |
| cci:persistentvolume:get         | Grants permission to query a PersistentVolume.        | Read         | PersistentVolume *          | -             |
| cci:persistentvolume:update      | Grants permission to update a PersistentVolume.       | Write        | PersistentVolume *          | -             |
| cci:persistentvolume:delete      | Grants permission to delete a PersistentVolume.       | Write        | PersistentVolume *          | -             |
| cci:persistentvolumeclaim:list   | Grants permission to list all PersistentVolumeClaims. | List         | PersistentVolumeClaim *     | -             |
| cci:persistentvolumeclaim:create | Grants permission to create a PersistentVolumeClaim.  | Write        | PersistentVolumeClaim *     | -             |

| Action                           | Description                                          | Access Level | Resource Type (*: required) | Condition Key                         |
|----------------------------------|------------------------------------------------------|--------------|-----------------------------|---------------------------------------|
| cci:persistentvolumeclaim:get    | Grants permission to query a PersistentVolumeClaim.  | Read         | PersistentVolumeClaim *     | -                                     |
| cci:persistentvolumeclaim:update | Grants permission to update a PersistentVolumeClaim. | Write        | PersistentVolumeClaim *     | -                                     |
| cci:persistentvolumeclaim:delete | Grants permission to delete a PersistentVolumeClaim. | Write        | PersistentVolumeClaim *     | -                                     |
| cci:storageclass:list            | Grants permission to list all StorageClasses.        | List         | -                           | -                                     |
| cci:deployment:list              | Grants permission to list all Deployments.           | List         | Deployment *                | -                                     |
| cci:deployment:create            | Grants permission to create a Deployment.            | Write        | Deployment *                | <a href="#">cci:AssociatePublicIp</a> |
| cci:deployment:get               | Grants permission to query a Deployment.             | Read         | Deployment *                | -                                     |
| cci:deployment:delete            | Grants permission to delete a Deployment.            | Write        | Deployment *                | -                                     |
| cci:deployment:update            | Grants permission to update a Deployment.            | Write        | Deployment *                | <a href="#">cci:AssociatePublicIp</a> |
| cci:service:list                 | Grants permission to list all Services.              | List         | Service *                   | -                                     |
| cci:service:create               | Grants permission to create a Service.               | Write        | Service *                   | -                                     |
| cci:service:get                  | Grants permission to query a Service.                | Read         | Service *                   | -                                     |

| Action                                | Description                                             | Access Level | Resource Type (*: required) | Condition Key |
|---------------------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------|
| cci:service:delete                    | Grants permission to delete a Service.                  | Write        | Service *                   | -             |
| cci:service:update                    | Grants permission to update a Service.                  | Write        | Service *                   | -             |
| cci:horizontalpodautoscaler:list      | Grants permission to list all HorizontalPodAutoscalers. | List         | -                           | -             |
| cci:horizontalpodautoscaler:create    | Grants permission to create a HorizontalPodAutoscaler.  | Write        | -                           | -             |
| cci:horizontalpodautoscaler:get       | Grants permission to query a HorizontalPodAutoscaler.   | Read         | -                           | -             |
| cci:horizontalpodautoscaler:delete    | Grants permission to delete a HorizontalPodAutoscaler.  | Write        | -                           | -             |
| cci:horizontalpodautoscaler:update    | Grants permission to update a HorizontalPodAutoscaler.  | Write        | -                           | -             |
| cci::updateobservabilityconfiguration | Grants permission to update ObservabilityConfiguration. | Write        | -                           | -             |
| cci::getobservabilityconfiguration    | Grants permission to query ObservabilityConfiguration.  | Read         | -                           | -             |
| cci:poolbinding:list                  | Grants permissions to list all PoolBindings.            | List         | -                           | -             |

| Action                 | Description                                | Access Level | Resource Type (*: required) | Condition Key |
|------------------------|--------------------------------------------|--------------|-----------------------------|---------------|
| cci:poolbinding:create | Grants permission to create a PoolBinding. | Write        | -                           | -             |
| cci:poolbinding:get    | Grants permissions to query a PoolBinding. | Read         | -                           | -             |
| cci:poolbinding:delete | Grants permission to delete a PoolBinding  | Write        | -                           | -             |

Each API of CCI usually supports one or more actions. [Table 3-77](#) lists the supported actions and dependencies.

**Table 3-77** Actions and dependencies supported by CCI APIs

| API                                                      | Action               | Dependencies |
|----------------------------------------------------------|----------------------|--------------|
| GET /apis/ci/v2/namespaces                               | cci:namespace:list   | -            |
| POST /apis/ci/v2/namespaces                              | cci:namespace:create | -            |
| GET /apis/ci/v2/namespaces/{name}                        | cci:namespace:get    | -            |
| DELETE /apis/ci/v2/namespaces/{name}                     | cci:namespace:delete | -            |
| GET /apis/ci/v2/namespaces/{namespace}/configmaps        | cci:configmap:list   | -            |
| POST /apis/ci/v2/namespaces/{namespace}/configmaps       | cci:configmap:create | -            |
| GET /apis/ci/v2/namespaces/{namespace}/configmaps/{name} | cci:configmap:get    | -            |



| API                                                                          | Action               | Dependencies |
|------------------------------------------------------------------------------|----------------------|--------------|
| PUT /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>configmaps/{name}        | cce:configmap:update | -            |
| DELETE /<br>apis/cce/v2/<br>namespaces/<br>{namespace}/<br>configmaps/{name} | cce:configmap:delete | -            |
| GET /apis/cce/v2/<br>namespaces/<br>{namespace}/pods                         | cce:pod:list         | -            |
| POST /apis/cce/v2/<br>namespaces/<br>{namespace}/pods                        | cce:pod:create       | -            |
| GET /apis/cce/v2/<br>namespaces/<br>{namespace}/pods/<br>{name}              | cce:pod:get          | -            |
| PUT /apis/cce/v2/<br>namespaces/<br>{namespace}/pods/<br>{name}              | cce:pod:update       | -            |
| DELETE /<br>apis/cce/v2/<br>namespaces/<br>{namespace}/pods/<br>{name}       | cce:pod:delete       | -            |
| PATCH /apis/cce/v2/<br>namespaces/<br>{namespace}/pods/<br>{name}            | cce:pod:update       | -            |
| GET /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>secrets                  | cce:secret:list      | -            |
| POST /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>secrets                 | cce:secret:create    | -            |

| API                                                                            | Action             | Dependencies |
|--------------------------------------------------------------------------------|--------------------|--------------|
| GET /apis/ccl/v2/<br>namespaces/<br>{namespace}/<br>secrets/{name}             | cci:secret:get     | -            |
| PUT /apis/ccl/v2/<br>namespaces/<br>{namespace}/<br>secrets/{name}             | cci:secret:update  | -            |
| DELETE /<br>apis/ccl/v2/<br>namespaces/<br>{namespace}/<br>secrets/{name}      | cci:secret:delete  | -            |
| GET /apis/<br>yangtse/v2/<br>namespaces/<br>{namespace}/<br>networks           | cci:network:list   | -            |
| POST /apis/<br>yangtse/v2/<br>namespaces/<br>{namespace}/<br>networks          | cci:network:create | -            |
| GET /apis/<br>yangtse/v2/<br>namespaces/<br>{namespace}/<br>networks/{name}    | cci:network:get    | -            |
| PUT /apis/<br>yangtse/v2/<br>namespaces/<br>{namespace}/<br>networks/{name}    | cci:network:update | -            |
| DELETE /apis/<br>yangtse/v2/<br>namespaces/<br>{namespace}/<br>networks/{name} | cci:network:delete | -            |
| POST /apis/ccl/v2/<br>namespaces/<br>{namespace}/pods/<br>{name}/exec          | cci:pod:exec       | -            |

| API                                                                                    | Action                                | Dependencies |
|----------------------------------------------------------------------------------------|---------------------------------------|--------------|
| GET /apis/csi/v2/<br>namespaces/<br>{namespace}/pods/<br>{name}/log                    | csi:pod:getLog                        | -            |
| GET /apis/csi/v2/<br>persistentvolumes                                                 | csi:persistentvolume:list             | -            |
| POST /apis/csi/v2/<br>persistentvolumes                                                | csi:persistentvolume:create           | -            |
| GET /apis/csi/v2/<br>persistentvolumes/<br>{name}                                      | csi:persistentvolume:get              | -            |
| PUT /apis/csi/v2/<br>persistentvolumes/<br>{name}                                      | csi:persistentvolume:update           | -            |
| DELETE /<br>apis/csi/v2/<br>persistentvolumes/<br>{name}                               | csi:persistentvolume:delete           | -            |
| GET /apis/csi/v2/<br>namespaces/<br>{namespace}/<br>persistentvolume-<br>claims        | csi:persistentvolume-<br>claim:list   | -            |
| POST /apis/csi/v2/<br>namespaces/<br>{namespace}/<br>persistentvolume-<br>claims       | csi:persistentvolume-<br>claim:create | -            |
| GET /apis/csi/v2/<br>namespaces/<br>{namespace}/<br>persistentvolume-<br>claims/{name} | csi:persistentvolume-<br>claim:get    | -            |
| PUT /apis/csi/v2/<br>namespaces/<br>{namespace}/<br>persistentvolume-<br>claims/{name} | csi:persistentvolume-<br>claim:update | -            |

| API                                                                                           | Action                                | Dependencies |
|-----------------------------------------------------------------------------------------------|---------------------------------------|--------------|
| DELETE /<br>apis/cce/v2/<br>namespaces/<br>{namespace}/<br>persistentvolume-<br>claims/{name} | cci:persistentvolume-<br>claim:delete | -            |
| GET /apis/cce/v2/<br>storageclasses                                                           | cci:storageclass:list                 | -            |
| GET /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>services                                  | cci:service:list                      | -            |
| POST /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>services                                 | cci:service:create                    | -            |
| GET /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>services/{name}                           | cci:service:get                       | -            |
| PUT /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>services/{name}                           | cci:service:update                    | -            |
| DELETE /<br>apis/cce/v2/<br>namespaces/<br>{namespace}/<br>services/{name}                    | cci:service:delete                    | -            |
| PATCH /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>services/{name}                         | cci:service:update                    | -            |
| GET /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>deployments                               | cci:deployment:list                   | -            |
| POST /apis/cce/v2/<br>namespaces/<br>{namespace}/<br>deployments                              | cci:deployment:create                 | -            |

| API                                                                                      | Action                                  | Dependencies |
|------------------------------------------------------------------------------------------|-----------------------------------------|--------------|
| GET /apis/ci/v2/<br>namespaces/<br>{namespace}/<br>deployments/<br>{name}                | cci:deployment:get                      | -            |
| PUT /apis/ci/v2/<br>namespaces/<br>{namespace}/<br>deployments/<br>{name}                | cci:deployment:update                   | -            |
| DELETE /<br>apis/ci/v2/<br>namespaces/<br>{namespace}/<br>deployments/<br>{name}         | cci:deployment:delete                   | -            |
| PATCH /apis/ci/v2/<br>namespaces/<br>{namespace}/<br>deployments/<br>{name}              | cci:deployment:update                   | -            |
| GET /apis/ci/v2/<br>namespaces/<br>{namespace}/<br>horizontalpodau-<br>toscalsers        | cci:horizontalpodautoscal-<br>er:list   | -            |
| POST /apis/ci/v2/<br>namespaces/<br>{namespace}/<br>horizontalpodau-<br>toscalsers       | cci:horizontalpodautoscal-<br>er:create | -            |
| GET /apis/ci/v2/<br>namespaces/<br>{namespace}/<br>horizontalpodau-<br>toscalsers/{name} | cci:horizontalpodautoscal-<br>er:get    | -            |
| PUT /apis/ci/v2/<br>namespaces/<br>{namespace}/<br>horizontalpodau-<br>toscalsers/{name} | cci:horizontalpodautoscal-<br>er:update | -            |

| API                                                                                           | Action                                | Dependencies |
|-----------------------------------------------------------------------------------------------|---------------------------------------|--------------|
| DELETE /apis/ccl/v2/namespaces/{namespace}/horizontalpodautoscalers/{name}                    | ccl:horizontalpodautoscaler:delete    | -            |
| PATCH /apis/ccl/v2/namespaces/{namespace}/horizontalpodautoscalers/{name}                     | ccl:horizontalpodautoscaler:update    | -            |
| PUT /v1/observabilityconfiguration                                                            | ccl::updateobservabilityconfiguration | -            |
| GET /v1/observabilityconfiguration                                                            | ccl::getobservabilityconfiguration    | -            |
| GET /apis/loadbalancer.network.openvessel.io/v1/namespaces/{namespace}/poolbindings           | ccl:poolbinding:list                  | -            |
| POST /apis/loadbalancer.network.openvessel.io/v1/namespaces/{namespace}/poolbindings          | ccl:poolbinding:create                | -            |
| GET /apis/loadbalancer.network.openvessel.io/v1/namespaces/{namespace}/poolbindings/{name}    | ccl:poolbinding:get                   | -            |
| DELETE /apis/loadbalancer.network.openvessel.io/v1/namespaces/{namespace}/poolbindings/{name} | ccl:poolbinding:delete                | -            |

**CAUTION**

If you want to disable OpenStack APIs in SCP policies, do not disable the **vpc:nativeSubnets:get** and **vpc:subnets:get** actions, or the network function of CCI will be abnormal.

## Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in [Table 3-78](#), the resource URN must be specified in the SCP statements using that action, and the SCP applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the SCP applies to all resources. You can also set condition keys in an SCP to define resource types.

The following table lists the resource types that you can define in SCP statements for CCI.

**Table 3-78** Resource types supported by CCI

| Resource Type          | URN                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------|
| Deployment             | cci:<region>:<account-id>:deployment:<namespace-name>/<deployment-name>                       |
| Secret                 | cci:<region>:<account-id>:secret:<namespace-name>/<secret-name>                               |
| Namespace              | cci:<region>:<account-id>:namespace:<namespace-name>                                          |
| Service                | cci:<region>:<account-id>:service:<namespace-name>/<service-name>                             |
| Network                | cci:<region>:<account-id>:network:<namespace-name>/<network-name>                             |
| PersistentVolume       | cci:<region>:<account-id>:persistentvolume:<persistentvolume-name>                            |
| ImageSnapshot          | cci:<region>:<account-id>:imagesnapshot:<imagesnapshot-name>                                  |
| ConfigMap              | cci:<region>:<account-id>:configmap:<namespace-name>/<configmap-name>                         |
| Pod                    | cci:<region>:<account-id>:pod:<namespace-name>/<pod-name>                                     |
| PersistentVolume-Claim | cci:<region>:<account-id>:persistentvolumeclaim:<namespace-name>/<persistentvolumeclaim-name> |

## Conditions

### Condition Key

A Condition element lets you specify conditions for when an SCP is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **cci:**) apply only to operations of the service. For details, see [Table 3-79](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An SCP can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by CCI

The following table lists the condition keys that you can define in custom SCP policies for CCI. You can include these condition keys to specify conditions for when your SCP policy is in effect.

**Table 3-79** Service-specific condition keys supported by CCI

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                                |
|--------------------------------|---------|-------------------------------|--------------------------------------------------------------------------------------------|
| cci:AssociatePublicIp          | Boolean | Single-valued                 | Filters the permission to bind EIPs to pods by the value of <b>cci:AssociatePublicIp</b> . |
| cci:ContainerName              | String  | Single-valued                 | Filters the permission to run commands in pods by container name.                          |



### 3.4.3 SWR Basic Edition

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by SWR, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by SWR, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for SWR.

**Table 3-80** Actions supported by SWR

| Action                        | Description                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|-------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| swr:namespace:createNamespace | Grants permission to create namespace for basic registry.  | Write        | namespace *                 | -                                     | -     |
| swr:namespace:deleteNamespace | Grants permission to delete namespace for basic registry.  | Write        | namespace *                 | -                                     | -     |
| swr:namespace:listNamespaces  | Grants permission to list namespaces for basic registry.   | List         | namespace *                 | -                                     | -     |
| swr:namespace:getNamespace    | Grants permission to get namespace for basic registry.     | Read         | namespace *                 | -                                     | -     |
| swr:repo:createRepo           | Grants permission to create repository for basic registry. | Write        | repo *                      | -                                     | -     |
|                               |                                                            |              | -                           | <a href="#">swr:AllowPublicAccess</a> |       |

| Action                   | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|--------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| swr:repo:deleteRepo      | Grants permission to delete repository for basic registry.        | Write        | repo *                      | -                                     | -     |
| swr:repo:listRepos       | Grants permission to list repositories for basic registry.        | List         | repo *                      | -                                     | -     |
| swr:repo:listSharedRepos | Grants permission to list basic repositories for basic registry.  | List         | repo *                      | -                                     | -     |
| swr:repo:getRepo         | Grants permission to get repository for basic registry.           | Read         | repo *                      | -                                     | -     |
| swr:repo:updateRepo      | Grants permission to update repository for basic registry.        | Write        | repo *                      | -                                     | -     |
|                          |                                                                   |              | -                           | <a href="#">swr:AllowPublicAccess</a> |       |
| swr:repo:deleteRepoTag   | Grants permission to delete tag of repository for basic registry. | Write        | repo *                      | -                                     | -     |
| swr:repo:createRepoTag   | Grants permission to create tag of repository for basic registry. | Write        | repo *                      | -                                     | -     |

| Action                    | Description                                                                  | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                        | Alias |
|---------------------------|------------------------------------------------------------------------------|-----------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repo:listRepoTags     | Grants permission to list tags of repository for basic registry.             | List                  | repo *                      | -                                                                                                                                                                                    | -     |
| swr:repo:createRepoDomain | Grants permission to create access domain of repository for basic registry.  | Permission_management | repo *<br>-                 | -<br><ul style="list-style-type: none"> <li>• <a href="#">swr:TargetAccountld</a></li> <li>• <a href="#">swr:TargetOrgPath</a></li> <li>• <a href="#">swr:TargetOrgld</a></li> </ul> | -     |
| swr:repo:deleteRepoDomain | Grants permission to delete access domain of repository for basic registry.  | Permission_management | repo *                      | -                                                                                                                                                                                    | -     |
| swr:repo:listRepoDomains  | Grants permission to list access domains of repository for basic registry.   | List                  | repo *                      | -                                                                                                                                                                                    | -     |
| swr:repo:getRepoDomain    | Grants permission to get access domain of repository for basic registry.     | Read                  | repo *                      | -                                                                                                                                                                                    | -     |
| swr:repo:updateRepoDomain | Grants permission to update access domain of repository for shared registry. | Permission_management | repo *                      | -                                                                                                                                                                                    | -     |

| Action                         | Description                                                                   | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                   | Alias |
|--------------------------------|-------------------------------------------------------------------------------|-----------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repo:createRepoShare       | Grants permission to create repo share rule of repository for basic registry. | Permission_management | repo *                      | -                                                                                                                                                                               |       |
|                                |                                                                               |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">swr:TargetAccountId</a></li> <li>• <a href="#">swr:TargetOrgPath</a></li> <li>• <a href="#">swr:TargetOrgId</a></li> </ul> |       |
| swr:repo:deleteRepoShare       | Grants permission to delete repo share rule of repository for basic registry. | Permission_management | repo *                      | -                                                                                                                                                                               | -     |
| swr:repo:listRepoShares        | Grants permission to list repo share rules of repository for basic registry.  | List                  | repo *                      | -                                                                                                                                                                               | -     |
| swr:repo:getRepoShare          | Grants permission to get repo share rule of repository for basic registry.    | Read                  | repo *                      | -                                                                                                                                                                               | -     |
| swr:repo:updateRepoShare       | Grants permission to update repo share rule of repository for basic registry. | Permission_management | repo *                      | -                                                                                                                                                                               | -     |
| swr:repo:createAutoSyncRepoJob | Grants permission to create auto sync repository job for basic registry.      | Write                 | repo *                      | -                                                                                                                                                                               |       |
|                                |                                                                               |                       | -                           | <a href="#">swr:TargetRegion</a>                                                                                                                                                |       |

| Action                           | Description                                                                | Access Level | Resource Type (*: required) | Condition Key    | Alias |
|----------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|------------------|-------|
| swr:repo:createManualSyncRepoJob | Grants permission to create manual sync repository job for basic registry. | Write        | repo *                      | -                | -     |
|                                  |                                                                            |              | -                           | swr:TargetRegion |       |
| swr:repo:deleteAutoSyncRepoJob   | Grants permission to delete auto sync repository job for basic registry.   | Write        | repo *                      | -                | -     |
| swr:repo:listAutoSyncRepoJobs    | Grants permission to list auto sync repository jobs for basic registry.    | List         | repo *                      | -                | -     |
| swr:repo:getSyncRepoJobInfo      | Grants permission to get auto sync repository job info for basic registry. | Read         | repo *                      | -                | -     |
| swr:repo:createTrigger           | Grants permission to create trigger for basic registry.                    | Write        | repo *                      | -                | -     |
| swr:repo:deleteTrigger           | Grants permission to delete trigger for basic registry.                    | Write        | repo *                      | -                | -     |
| swr:repo:listTriggers            | Grants permission to list triggers for basic registry.                     | List         | repo *                      | -                | -     |

| Action                          | Description                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| swr:repo:getTrigger             | Grants permission to get trigger for basic registry.              | Read         | repo *                      | -             | -     |
| swr:repo:updateTrigger          | Grants permission to update trigger for basic registry.           | Write        | repo *                      | -             | -     |
| swr:repo:createRetention        | Grants permission to create retention for basic registry.         | Write        | repo *                      | -             | -     |
| swr:repo:deleteRetention        | Grants permission to delete retention for basic registry.         | Write        | repo *                      | -             | -     |
| swr:repo:listRetentionHistories | Grants permission to list retention histories for basic registry. | List         | repo *                      | -             | -     |
| swr:repo:listRetentions         | Grants permission to list retentions for basic registry.          | List         | repo *                      | -             | -     |
| swr:repo:getRetention           | Grants permission to get retention for basic registry.            | Read         | repo *                      | -             | -     |
| swr:repo:updateRetention        | Grants permission to update retention for basic registry.         | Write        | repo *                      | -             | -     |

| Action                              | Description                                                                       | Access Level          | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------------|-----------------------------------------------------------------------------------|-----------------------|-----------------------------|---------------|-------|
| swr::createLoginSecret              | Grants permission to create login secret for basic registry.                      | Write                 | -                           | -             | -     |
| swr::createAuthorizationToken       | Grants permission to create a new temporary access credential for basic registry. | Write                 | -                           | -             | -     |
| swr::listQuotas                     | Grants permission to list quotas for basic registry.                              | List                  | -                           | -             | -     |
| swr::getDomainOverview              | Grants permission to get overview of domain for basic registry.                   | Read                  | -                           | -             | -     |
| swr::getDomainResourceReports       | Grants permission to get down flow reports of domain for basic registry.          | Read                  | -                           | -             | -     |
| swr:namespace:multipartUpload       | Grants permission to multipart upload for basic registry.                         | Write                 | namespace *                 | -             | -     |
| swr:namespace:createNamespaceAccess | Grants permission to create namespace access for basic registry.                  | Permission_management | namespace *                 | -             | -     |



| Action                              | Description                                                       | Access Level          | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------------|-------------------------------------------------------------------|-----------------------|-----------------------------|---------------|-------|
| swr:namespace:deleteNamespaceAccess | Grants permission to delete namespace access for basic registry.  | Permission_management | namespace *                 | -             | -     |
| swr:namespace:getNamespaceAccess    | Grants permission to get namespace access for basic registry.     | Read                  | namespace *                 | -             | -     |
| swr:namespace:updateNamespaceAccess | Grants permission to update namespace access for basic registry.  | Permission_management | namespace *                 | -             | -     |
| swr:repo:createRepoAccess           | Grants permission to create repository access for basic registry. | Permission_management | repo *                      | -             | -     |
| swr:repo:deleteRepoAccess           | Grants permission to delete repository access for basic registry. | Permission_management | repo *                      | -             | -     |
| swr:repo:getRepoAccess              | Grants permission to get repository access for basic registry.    | Read                  | repo *                      | -             | -     |
| swr:repo:updateRepoAccess           | Grants permission to update repository access for basic registry. | Permission_management | repo *                      | -             | -     |

| Action              | Description                                                      | Access Level | Resource Type (*: required) | Condition Key           | Alias |
|---------------------|------------------------------------------------------------------|--------------|-----------------------------|-------------------------|-------|
| swr:repo:upload     | Grants permission to upload repository for basic registry.       | Write        | repo *                      | -                       | -     |
|                     |                                                                  |              | -                           | swr:AllowCredentialType |       |
| swr:repo:download   | Grants permission to download repository for basic registry.     | Read         | repo *                      | swr:RepositoryIsPublic  | -     |
|                     |                                                                  |              | -                           | swr:AllowCredentialType |       |
| swr:repo:getRepoTag | Grants permission to query tag of repository for basic registry. | Read         | repo *                      | -                       | -     |

Each API of SWR usually supports one or more actions. [Table 3-81](#) lists the supported actions and dependencies.

**Table 3-81** Actions and dependencies supported by SWR APIs

| API                                          | Action                        | Dependencies |
|----------------------------------------------|-------------------------------|--------------|
| POST /v2/manage/namespaces                   | swr:namespace:createNamespace | -            |
| DELETE /v2/manage/namespaces/{namespace}     | swr:namespace:deleteNamespace | -            |
| GET /v2/manage/namespaces                    | swr:namespace:listNamespaces  | -            |
| GET /v2/manage/namespaces/{namespace}        | swr:namespace:getNamespace    | -            |
| POST /v2/manage/namespaces/{namespace}/repos | swr:repo:createRepo           | -            |

| API                                                                                                 | Action                    | Dependencies |
|-----------------------------------------------------------------------------------------------------|---------------------------|--------------|
| DELETE /v2/<br>manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}                         | swr:repo:deleteRepo       | -            |
| GET /v2/manage/<br>repos                                                                            | swr:repo:listRepos        | -            |
| GET /v2/manage/<br>shared-repositories                                                              | swr:repo:listSharedRepos  | -            |
| GET /v2/manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}                                | swr:repo:getRepo          | -            |
| PATCH /v2/manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}                              | swr:repo:updateRepo       | -            |
| DELETE /v2/<br>manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}/tags/<br>{tag}          | swr:repo:deleteRepoTag    | -            |
| POST /v2/manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}/tags                          | swr:repo:createRepoTag    | -            |
| GET /v2/manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}/tags                           | swr:repo:listRepoTags     | -            |
| POST /v2/manage/<br>namespaces/<br>{namespace}/<br>repositories/<br>{repository}/access-<br>domains | swr:repo:createRepoDomain | -            |

| API                                                                                               | Action                    | Dependencies |
|---------------------------------------------------------------------------------------------------|---------------------------|--------------|
| DELETE /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain} | swr:repo:deleteRepoDomain | -            |
| GET /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains                    | swr:repo:listRepoDomains  | -            |
| GET /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}    | swr:repo:getRepoDomain    | -            |
| PATCH /v2/manage/namespaces/{namespace}/repositories/{repository}/access-domains/{access_domain}  | swr:repo:updateRepoDomain | -            |
| POST /v2/manage/namespaces/{namespace}/repos/{repository}/shares                                  | swr:repo:createRepoShare  | -            |
| DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id}                     | swr:repo:deleteRepoShare  | -            |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/shares                                   | swr:repo:listRepoShares   | -            |

| API                                                                          | Action                           | Dependencies                                                                                                                       |
|------------------------------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id}   | swr:repo:getRepoShare            | -                                                                                                                                  |
| PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/shares/{share_id} | swr:repo:updateRepoShare         | -                                                                                                                                  |
| POST /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo          | swr:repo:createAutoSyncRepoJob   | <ul style="list-style-type: none"> <li>• swr::createLoginSecret</li> <li>• swr:repo:download</li> <li>• swr:repo:upload</li> </ul> |
| POST /v2/manage/namespaces/{namespace}/repos/{repository}/sync_images        | swr:repo:createManualSyncRepoJob | <ul style="list-style-type: none"> <li>• swr::createLoginSecret</li> <li>• swr:repo:download</li> <li>• swr:repo:upload</li> </ul> |
| DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo        | swr:repo:deleteAutoSyncRepoJob   | -                                                                                                                                  |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/sync_repo           | swr:repo:listAutoSyncRepoJobs    | -                                                                                                                                  |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/sync_job            | swr:repo:getSyncRepoJobInfo      | -                                                                                                                                  |
| POST /v2/manage/namespaces/{namespace}/repos/{repository}/triggers           | swr:repo:createTrigger           | -                                                                                                                                  |

| API                                                                                   | Action                          | Dependencies |
|---------------------------------------------------------------------------------------|---------------------------------|--------------|
| DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}        | swr:repo:deleteTrigger          | -            |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/triggers                     | swr:repo:listTriggers           | -            |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}           | swr:repo:getTrigger             | -            |
| PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}         | swr:repo:updateTrigger          | -            |
| POST /v2/manage/namespaces/{namespace}/repos/{repository}/retentions                  | swr:repo:createRetention        | -            |
| DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id} | swr:repo:deleteRetention        | -            |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/histories         | swr:repo:listRetentionHistories | -            |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions                   | swr:repo:listRetentions         | -            |

| API                                                                                                      | Action                                  | Dependencies                       |
|----------------------------------------------------------------------------------------------------------|-----------------------------------------|------------------------------------|
| GET /v2/manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}/<br>retentions/<br>{retention_id}   | swr:repo:getRetention                   | -                                  |
| PATCH /v2/manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}/<br>retentions/<br>{retention_id} | swr:repo:updateRetention                | -                                  |
| POST /v2/manage/<br>utils/secret                                                                         | swr::createLoginSecret                  | -                                  |
| POST /v2/manage/<br>utils/<br>authorizationtoken                                                         | swr::createAuthorizationTo-<br>ken      | sts::createServiceBearerTo-<br>ken |
| GET /v2/manage/<br>projects/<br>{project_id}/quotas                                                      | swr::listQuotas                         | -                                  |
| GET /v2/manage/<br>overview                                                                              | swr::getDomainOverview                  | -                                  |
| GET /v2/manage/<br>reports/<br>{resource_type}/<br>{frequency}                                           | swr::getDomainResourceRe-<br>ports      | -                                  |
| POST /v2/manage/<br>namespaces/<br>{namespace}/access                                                    | swr:namespace:createName<br>spaceAccess | -                                  |
| DELETE /v2/<br>manage/<br>namespaces/<br>{namespace}/access                                              | swr:namespace:deleteName<br>spaceAccess | -                                  |
| GET /v2/manage/<br>namespaces/<br>{namespace}/access                                                     | swr:namespace:getNamesp<br>aceAccess    | -                                  |
| PATCH /v2/manage/<br>namespaces/<br>{namespace}/access                                                   | swr:namespace:updateNam<br>espaceAccess | -                                  |
| POST /v2/manage/<br>namespaces/<br>{namespace}/repos/<br>{repository}/access                             | swr:repo:createRepoAccess               | -                                  |

| API                                                                | Action                    | Dependencies |
|--------------------------------------------------------------------|---------------------------|--------------|
| DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/access | swr:repo:deleteRepoAccess | -            |
| GET /v2/manage/namespaces/{namespace}/repos/{repository}/access    | swr:repo:getRepoAccess    | -            |
| PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/access  | swr:repo:updateRepoAccess | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-82](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for SWR.

**Table 3-82** Resource types supported by SWR

| Resource Type | URN                                                         |
|---------------|-------------------------------------------------------------|
| repo          | swr:<region>:<account-id>:repo:<namespace-name>/<repo-name> |
| namespace     | swr:<region>:<account-id>:namespace:<namespace-name>        |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the



system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).

- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, swr) apply only to operations of the xx service. For details, see [Table 3-83](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

#### Service-specific condition keys supported by SWR

The following table lists the condition keys that you can define in identity policies for SWR. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-83** Service-specific condition keys supported by SWR

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                            |
|--------------------------------|---------|-------------------------------|--------------------------------------------------------|
| swr:TargetOrgPath              | string  | Single-valued                 | Filters access by destination's OrgPath.               |
| swr:TargetOrgId                | string  | Single-valued                 | Filters access by destination's OrgId.                 |
| swr:TargetAccountId            | string  | Single-valued                 | Filters access by destination's AccountId.             |
| swr:AllowPublicAccess          | boolean | Single-valued                 | Filters access by the repos that can be set to public. |
| swr:TargetRegion               | string  | Single-valued                 | Filters access by target region.                       |
| swr:AllowCredential-Type       | string  | Single-valued                 | Filters access by the credential type.                 |
| swr:RepositoryIsPublic         | boolean | Single-valued                 | Filters access by public repositories.                 |

### 3.4.4 SWR Enterprise Edition

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by SWR, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by SWR, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for SWR.

**Table 3-84** Actions supported by SWR

| Action                             | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:createImmutableRule | Grants permission to create immutableRule for edition instance. | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:deleteImmutableRule | Grants permission to delete immutableRule for edition instance. | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listImmutableRules  | Grants permission to list immutableRule for edition instance.   | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:updateImmutableRule | Grants permission to update immutableRule for edition instance. | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listArtifacts       | Grants permission to query the artifact list.                   | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                             | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:getArtifact         | Grants permission to query the policy of resource instance.          | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:deleteArtifact      | Grants permission to delete a artifact.                              | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listAccessories     | Grants permission to query the accessory list.                       | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:getArtifactAddition | Grants permission to query the addition information of a artifact.   | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:getConfigurations     | Grants permission to query the configurations of resource instance.  | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:updateConfigurations  | Grants permission to update the configurations of resource instance. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                 | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:listResourceInstances     | Grants permission to query the list of resource instance.  | List         | instance *                  | -                                                                                                                                                  | -     |
|                                        |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul>              | -     |
| swr:instance:getResourceInstancesCount | Grants permission to query the count of resource instance. | Read         | instance *                  | -                                                                                                                                                  | -     |
|                                        |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul>              | -     |
| swr:instance:createResourceTags        | Grants permission to create resource tags in batch.        | Tagging      | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                        |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              | -     |
| swr:instance:deleteResourceTags        | Grants permission to delete resource tags in batch.        | Tagging      | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                        |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              | -     |
| swr:instance:getProjectTags            | Grants permission to query the resource tags of project.   | Read         | -                           | -                                                                                                                                                  | -     |

| Action                       | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                       | Alias |
|------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:getResourceTags | Grants permission to query the resource tags of resource.            | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                  | -     |
| swr:instance:create          | Grants permission to create an enterprise edition instance.          | Write        | instance *                  | -                                                                                                                                                                                                                                                                                                                   | -     |
|                              |                                                                      |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">swr:VpcId</a></li> <li>• <a href="#">swr:SubnetId</a></li> <li>• <a href="#">swr:EnableObsEncrypt</a></li> </ul> | -     |
| swr:instance:list            | Grants permission to query the list of enterprise edition instances. | List         | instance *                  | -                                                                                                                                                                                                                                                                                                                   | -     |
| swr:instance:get             | Grants permission to query an enterprise edition instance.           | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                  | -     |
| swr:instance:delete          | Grants permission to delete an enterprise edition instance.          | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                  | -     |

| Action                         | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:getAuditLogs      | Grants permission to query the audit logs of an enterprise edition instance. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:getStatistics     | Grants permission to query the statistics of an enterprise edition instance. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:listJobs          | Grants permission to query the list of jobs.                                 | List         | instance *                  | -                                                                                                                                                  | -     |
| swr:instance:getJobs           | Grants permission to query a job.                                            | Read         | instance *                  | -                                                                                                                                                  | -     |
| swr:instance:deleteJob         | Grants permission to delete a job.                                           | Write        | instance *                  | -                                                                                                                                                  | -     |
| swr:repository:createNamespace | Grants permission to create a namespace.                                     | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                |                                                                              |              | -                           | <a href="#">swr:EnablePublicNamespace</a>                                                                                                          | -     |
| swr:repository:listNamespaces  | Grants permission to query the list of namespace.                            | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                          | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:getNamespace     | Grants permission to query an namespace.                      | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:updateNamespace  | Grants permission to update an namespace.                     | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                 |                                                               |              | -                           | <a href="#">swr:EnablePublicNameSpace</a>                                                                                                          | -     |
| swr:repository:deleteNamespace  | Grants permission to delete an namespace.                     | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listRepositories | Grants permission to query the list of artifact repositories. | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:getRepository    | Grants permission to query an artifact repository.            | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:updateRepository | Grants permission to update an artifact repository.           | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |



| Action                               | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:deleteRepository      | Grants permission to delete an artifact repository.           | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listTags              | Grants permission to query the tag list.                      | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:getTag                | Grants permission to query the details of a tag.              | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:deleteTag             | Grants permission to delete a tag.                            | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:getTagAddition        | Grants permission to query the addition information of a tag. | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:createRetentionPolicy | Grants permission to create an image tag retention policy.    | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                       | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:listRetentionPolicies         | Grants permission to query the list of image tag retention policies.     | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:getRetentionPolicy            | Grants permission to query the details of an image tag retention policy. | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:updateRetentionPolicy         | Grants permission to update an image tag retention policy.               | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:deleteRetentionPolicy         | Grants permission to delete an image tag retention policy.               | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:executeRetentionPolicy        | Grants permission to apply an image tag retention policy.                | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listRetentionPolicyExecutions | Grants permission to query the history of image tag retention events.    | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                         | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:listRetentionPolicyExecTasks    | Grants permission to query the list of image tag retention tasks.    | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listRetentionPolicyExecSubTasks | Grants permission to query the list of image tag retention subtasks. | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:createWebhook                   | Grants permission to create a trigger.                               | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listWebhooks                    | Grants permission to query the list of triggers.                     | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:getWebhook                      | Grants permission to query the details of a trigger.                 | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:updateWebhook                   | Grants permission to edit a trigger.                                 | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                         | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:deleteWebhook   | Grants permission to delete a trigger.                            | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listWebhookJobs | Grants permission to query the list of triggers.                  | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:createRegistry    | Grants permission to create a destination registry.               | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:listRegistries    | Grants permission to query the list of destination registries.    | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:getRegistry       | Grants permission to query the details of a destination registry. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:updateRegistry    | Grants permission to edit a destination registry.                 | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                               | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                  | Alias |
|--------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:deleteRegistry          | Grants permission to delete a destination registry.             | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                             | -     |
| swr:instance:createReplicationPolicy | Grants permission to create a replication policy.               | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">swr:TargetRegion</a></li> <li>• <a href="#">swr:SourceRegion</a></li> <li>• <a href="#">swr:TargetUrls</a></li> <li>• <a href="#">swr:SourceUrls</a></li> </ul> | -     |
| swr:instance:listReplicationPolicies | Grants permission to query the replication policy list.         | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                             | -     |
| swr:instance:getReplicationPolicy    | Grants permission to query the details of a replication policy. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                             | -     |

| Action                                       | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                  | Alias |
|----------------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:updateReplicationPolicy         | Grants permission to edit a replication policy.               | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">swr:TargetRegion</a></li> <li>• <a href="#">swr:SourceRegion</a></li> <li>• <a href="#">swr:TargetUrls</a></li> <li>• <a href="#">swr:SourceUrls</a></li> </ul> | -     |
| swr:instance:deleteReplicationPolicy         | Grants permission to delete a replication policy.             | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                             | -     |
| swr:instance:executeReplicationPolicy        | Grants permission to apply a replication policy.              | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                             | -     |
| swr:instance:stopReplicationPolicyExecution  | Grants permission to stop the history of replication events.  | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                             | -     |
| swr:instance:listReplicationPolicyExecutions | Grants permission to query the history of replication events. | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                             | -     |

| Action                                         | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:listReplicationPolicyExecTasks    | Grants permission to query the list of replication tasks.      | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:listReplicationPolicyExecSubTasks | Grants permission to query the list of a replication subtasks. | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:createSignPolicy                | Grants permission to create a signing policy.                  | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listSignPolicies                | Grants permission to query the signing policy list.            | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:getSignPolicy                   | Grants permission to query the details of a signing policy.    | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:updateSignPolicy                | Grants permission to edit a signing policy.                    | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                    | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:repository:deleteSignPolicy           | Grants permission to delete a signing policy.                       | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:executeSignPolicy          | Grants permission to apply a signing policy.                        | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listSignPolicyExecutions   | Grants permission to query the history of signing events.           | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listSignPolicyExecTasks    | Grants permission to query the list of signing tasks.               | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listSignPolicyExecSubTasks | Grants permission to query the list of signing subtasks.            | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:updateEndpointPolicy         | Grants permission to update the whitelist of public network access. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |



| Action                                  | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:updateEndpointPolicyStatus | Grants permission to update the whitelist of public network access status. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:getEndpointPolicy          | Grants permission to query the whitelist of public network access.         | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:createInternalEndpoint     | Grants permission to create an internal endpoint.                          | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                         |                                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">swr:VpcId</a></li> <li>• <a href="#">swr:SubnetId</a></li> </ul>                              | -     |
| swr:instance:getInternalEndpoint        | Grants permission to get an internal endpoint.                             | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:deleteInternalEndpoint     | Grants permission to delete an internal endpoint.                          | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                             | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                        | Alias |
|------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:listInternalEndpoints | Grants permission to query the list of internal endpoints.                | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                   | -     |
| swr:repository:uploadArtifact      | Grants permission to upload an artifact.                                  | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                   | -     |
| swr:repository:downloadArtifact    | Grants permission to download an artifact.                                | Read         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">swr:RepositoryIsPublic</a></li> </ul> | -     |
| swr:instance:createTempCredential  | Grants permission to create a temporary access credential.                | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                   | -     |
| swr:instance:createLTCredential    | Grants permission to create an access credential with long-term validity. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                   | -     |

| Action                          | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:updateLTCredential | Grants permission to enable/disable an access credential with long-term validity. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:listLTCredentials  | Grants permission to query the list of long-term validity.                        | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:deleteLTCredential | Grants permission to delete an access credential with long-term validity.         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:addDomainName      | Grants permission to add a domain name.                                           | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:deleteDomainName   | Grants permission to delete a domain name.                                        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:updateDomainName   | Grants permission to update a domain name.                                        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                             | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| swr:instance:listDomainNames       | Grants permission to query the list of domain name.          | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:listCatalog         | Grants permission to query the list of catalog.              | List         | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:instance:listAllArtifacts      | Grants permission to query the list of instance artifacts.   | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| swr:repository:startManualScanning | Grant permission for manual initiation of artifact scanning. | Write        | repository *                | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

Each API of SWR usually supports one or more actions. [Table 3-85](#) lists the supported actions and dependencies.

**Table 3-85** Actions and dependencies supported by SWR APIs

| API                                                                                                                                       | Action                         | Dependencies |
|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts                         | swr:repository:listArtifacts   | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts/{reference}             | swr:repository:getArtifact     | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts/{reference}          | swr:repository:deleteArtifact  | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts/{reference}/accessories | swr:repository:listAccessories | -            |

| API                                                                                                                                                | Action                                 | Dependencies |
|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts/{reference}/additions/{addition} | swr:repository:getArtifactAddition     | -            |
| GET /v2/{project_id}/instances/{instance_id}/configurations                                                                                        | swr:instance:getConfigurations         | -            |
| PUT /v2/{project_id}/instances/{instance_id}/configurations                                                                                        | swr:instance:updateConfigurations      | -            |
| POST /v2/{project_id}/{resource_type}/resource-instances/filter                                                                                    | swr:instance:listResourceInstances     | -            |
| POST /v2/{project_id}/{resource_type}/resource-instances/count                                                                                     | swr:instance:getResourceInstancesCount | -            |
| POST /v2/{project_id}/{resource_type}/{resource_id}/tags/create                                                                                    | swr:instance:createResourceTags        | -            |
| DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/delete                                                                                  | swr:instance:deleteResourceTags        | -            |
| GET /v2/{project_id}/instances/tags                                                                                                                | swr:instance:getProjectTags            | -            |

| API                                                      | Action                         | Dependencies |
|----------------------------------------------------------|--------------------------------|--------------|
| GET /v2/{project_id}/{resource_type}/{resource_id}/tags  | swr:instance:getResourceTags   | -            |
| POST /v2/{project_id}/instances                          | swr:instance:create            | -            |
| GET /v2/{project_id}/instances                           | swr:instance:list              | -            |
| GET /v2/{project_id}/instances/{instance_id}             | swr:instance:get               | -            |
| DELETE /v2/{project_id}/instances/{instance_id}          | swr:instance:delete            | -            |
| GET /v2/{project_id}/instances/{instance_id}/audit-logs  | swr:instance:getAuditLogs      | -            |
| GET /v2/{project_id}/instances/{instance_id}/statistics  | swr:instance:getStatistics     | -            |
| GET /v2/{project_id}/jobs                                | swr:instance:listJobs          | -            |
| DELETE /v2/{project_id}/jobs/{job_id}                    | swr:instance:deleteJob         | -            |
| POST /v2/{project_id}/instances/{instance_id}/namespaces | swr:repository:createNamespace | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces  | swr:repository:listNamespaces  | -            |

| API                                                                                                     | Action                          | Dependencies |
|---------------------------------------------------------------------------------------------------------|---------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}                                | swr:repository:getNamespace     | -            |
| PUT /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}                                | swr:repository:updateNamespace  | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}                             | swr:repository:deleteNamespace  | -            |
| GET /v2/{project_id}/instances/{instance_id}/repositories                                               | swr:repository:listRepositories | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name} | swr:repository:getRepository    | -            |
| PUT /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name} | swr:repository:updateRepository | -            |



| API                                                                                                                                                | Action                               | Dependencies |
|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| DELETE /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}                                         | swr:repository:deleteRepository      | -            |
| GET /v2/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/tags                                                    | swr:repository:listTags              | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts/{reference}/additions/{addition} | swr:repository:getTagAddition        | -            |
| POST /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies                                                       | swr:repository:createRetentionPolicy | -            |
| GET /v2/{project_id}/instances/{instance_id}/retention/policies                                                                                    | swr:repository:listRetentionPolicies | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies/{policy_id}                                            | swr:repository:getRetentionPolicy    | -            |

| API                                                                                                                                     | Action                                       | Dependencies |
|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|--------------|
| PUT /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies/{policy_id}                                 | swr:repository:updateRetentionPolicy         | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies/{policy_id}                              | swr:repository:deleteRetentionPolicy         | -            |
| POST /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies/{policy_id}/executions                     | swr:repository:executeRetentionPolicy        | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies/{policy_id}/executions                      | swr:repository:listRetentionPolicyExecutions | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies/{policy_id}/executions/{execution_id}/tasks | swr:repository:listRetentionPolicyExecTasks  | -            |

| API                                                                                                                                                        | Action                                         | Dependencies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/retention/policies/{policy_id}/executions/{execution_id}/tasks/{task_id}/subtasks | swr:repository:listRetentionPolicyExecSubTasks | -            |
| POST /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/webhook/policies                                                                 | swr:repository:createWebhook                   | -            |
| GET /v2/{project_id}/instances/{instance_id}/webhook/policies                                                                                              | swr:repository:listWebhooks                    | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/webhook/policies/{policy_id}                                                      | swr:repository:getWebhook                      | -            |
| PUT /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/webhook/policies/{policy_id}                                                      | swr:repository:updateWebhook                   | -            |

| API                                                                                                            | Action                             | Dependencies |
|----------------------------------------------------------------------------------------------------------------|------------------------------------|--------------|
| DELETE /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/webhook/policies/{policy_id}       | swr:repository:deleteWebhook       | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/webhook/policies/{policy_id}/jobs     | swr:repository:listWebhookJobs     | -            |
| POST /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/immutablerules                       | swr:repository:createImmutableRule | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/immutablerules/{immutable_rule_id} | swr:repository:deleteImmutableRule | -            |
| GET /v2/{project_id}/instances/{instance_id}/immutablerules                                                    | swr:repository:listImmutableRules  | -            |
| PUT /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/immutablerules/{immutable_rule_id}    | swr:repository:updateImmutableRule | -            |

| API                                                                           | Action                               | Dependencies |
|-------------------------------------------------------------------------------|--------------------------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/registries                      | swr:instance:createRegistry          | -            |
| GET /v2/{project_id}/instances/{instance_id}/registries                       | swr:instance:listRegistries          | -            |
| GET /v2/{project_id}/instances/{instance_id}/registries/{registry_id}         | swr:instance:getRegistry             | -            |
| PUT /v2/{project_id}/instances/{instance_id}/registries/{registry_id}         | swr:instance:updateRegistry          | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/registries/{registry_id}      | swr:instance:deleteRegistry          | -            |
| POST /v2/{project_id}/instances/{instance_id}/replication/policies            | swr:instance:createReplicationPolicy | -            |
| GET /v2/{project_id}/instances/{instance_id}/replication/policies             | swr:instance:listReplicationPolicies | -            |
| GET /v2/{project_id}/instances/{instance_id}/replication/policies/{policy_id} | swr:instance:getReplicationPolicy    | -            |

| API                                                                                      | Action                                        | Dependencies |
|------------------------------------------------------------------------------------------|-----------------------------------------------|--------------|
| PUT /v2/{project_id}/instances/{instance_id}/replication/policies/{policy_id}            | swr:instance:updateReplicationPolicy          | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/replication/policies/{policy_id}         | swr:instance:deleteReplicationPolicy          | -            |
| POST /v2/{project_id}/instances/{instance_id}/replication/executions                     | swr:instance:executeReplicationPolicy         | -            |
| PUT /v2/{project_id}/instances/{instance_id}/replication/executions/{execution_id}       | swr:instance:stopReplicationPolicyExecution   | -            |
| GET /v2/{project_id}/instances/{instance_id}/replication/executions                      | swr:instance:listReplication-PolicyExecutions | -            |
| GET /v2/{project_id}/instances/{instance_id}/replication/executions/{execution_id}/tasks | swr:instance:listReplication-PolicyExecTasks  | -            |

| API                                                                                                         | Action                                          | Dependencies |
|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/replication/executions/{execution_id}/tasks/{task_id}/subtasks | swr:instance:listReplication-PolicyExecSubTasks | -            |
| POST /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies                | swr:repository:createSignPolicy                 | -            |
| GET /v2/{project_id}/instances/{instance_id}/signature/policies                                             | swr:repository:listSignPolicies                 | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies/{policy_id}     | swr:repository:getSignPolicy                    | -            |
| PUT /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies/{policy_id}     | swr:repository:updateSignPolicy                 | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies/{policy_id}  | swr:repository:deleteSignPolicy                 | -            |

| API                                                                                                                                                        | Action                                    | Dependencies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies/{policy_id}/executions                                        | swr:repository:executeSignPolicy          | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies/{policy_id}/executions                                         | swr:repository:listSignPolicyExecutions   | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies/{policy_id}/executions/{execution_id}/tasks                    | swr:repository:listSignPolicyExecTasks    | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/signature/policies/{policy_id}/executions/{execution_id}/tasks/{task_id}/subtasks | swr:repository:listSignPolicyExecSubTasks | -            |
| PUT /v2/{project_id}/instances/{instance_id}/endpoint-policy                                                                                               | swr:instance:updateEndpointPolicy         | -            |



| API                                                                                        | Action                                  | Dependencies |
|--------------------------------------------------------------------------------------------|-----------------------------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/endpoint-policy                              | swr:instance:updateEndpointPolicyStatus | -            |
| GET /v2/{project_id}/instances/{instance_id}/endpoint-policy                               | swr:instance:getEndpointPolicy          | -            |
| POST /v2/{project_id}/instances/{instance_id}/internal-endpoints                           | swr:instance:createInternalEndpoint     | -            |
| GET /v2/{project_id}/instances/{instance_id}/internal-endpoints/{internal_endpoints_id}    | swr:instance:getInternalEndpoint        | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/internal-endpoints/{internal_endpoints_id} | swr:instance:deleteInternalEndpoint     | -            |
| GET /v2/{project_id}/instances/{instance_id}/internal-endpoints                            | swr:instance:listInternalEndpoints      | -            |
| POST /v2/{project_id}/instances/{instance_id}/temp-credential                              | swr:instance:createTempCredential       | -            |
| POST /v2/{project_id}/instances/{instance_id}/long-term-credential                         | swr:instance:createLTCTCredential       | -            |

| API                                                                                   | Action                          | Dependencies    |
|---------------------------------------------------------------------------------------|---------------------------------|-----------------|
| PUT /v2/{project_id}/instances/{instance_id}/long-term-credentials/{credential_id}    | swr:instance:updateLTCredential | -               |
| GET /v2/{project_id}/instances/{instance_id}/long-term-credentials                    | swr:instance:listLTCredentials  | -               |
| DELETE /v2/{project_id}/instances/{instance_id}/long-term-credentials/{credential_id} | swr:instance:deleteLTCredential | -               |
| POST /v2/{project_id}/instances/{instance_id}/domainname                              | swr:instance:addDomainName      | scm:cert:export |
| DELETE /v2/{project_id}/instances/{instance_id}/domainname/{domainname_id}            | swr:instance:deleteDomainName   | -               |
| PUT /v2/{project_id}/instances/{instance_id}/domainname/{domainname_id}               | swr:instance:updateDomainName   | -               |
| GET /v2/{project_id}/instances/{instance_id}/domainname                               | swr:instance:listDomainNames    | -               |
| GET /v2/{project_id}/instances/{instance_id}/artifacts                                | swr:instance:listAllArtifacts   | -               |

| API                                                                                                                                           | Action                                     | Dependencies |
|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts/{reference}/scan           | swr:repository:startManualScanning         | -            |
| GET /v2/{project_id}/instances/{instance_id}/namespaces/{namespace_name}/repositories/{repository_name}/artifacts/{reference}/vulnerabilities | swr:repository:listArtifactVulnerabilities | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-86](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for SWR.

**Table 3-86** Resource types supported by SWR

| Resource Type | URN                                                                    |
|---------------|------------------------------------------------------------------------|
| repository    | swr:<region>:<account-id>:repository:<instance-name>/<repository-path> |
| instance      | swr:<region>:<account-id>:instance:<instance-name>                     |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, swr) apply only to operations of the xx service. For details, see **Table 3-87**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

#### Service-specific condition keys supported by SWR

The following table lists the condition keys that you can define in identity policies for SWR. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-87** Service-specific condition keys supported by SWR

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                         |
|--------------------------------|---------|-------------------------------|---------------------------------------------------------------------|
| swr:VpcId                      | string  | Single-valued                 | Filters access by user's VPC ID.                                    |
| swr:SubnetId                   | string  | Single-valued                 | Filters access by user's Subnet ID.                                 |
| swr:EnablePublicNameSpace      | boolean | Single-valued                 | Filters access by enterprise instance's namespace public attribute. |
| swr:EnableObsEncrypt           | boolean | Single-valued                 | Filters access by enterprise instance's obs bucket encrypted type.  |

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                            |
|--------------------------------|---------|-------------------------------|----------------------------------------|
| swr:TargetRegion               | string  | Single-valued                 | Filters access by target region.       |
| swr:SourceRegion               | string  | Single-valued                 | Filters access by source region.       |
| swr:TargetUrls                 | string  | Multivalued                   | Filters access by target url.          |
| swr:SourceUrls                 | string  | Multivalued                   | Filters access by source url.          |
| swr:RepositoryIsPublic         | boolean | Single-valued                 | Filters access by public repositories. |

## 3.5 Content Delivery & Edge Computing

### 3.5.1 Content Delivery Network (CDN)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CDN, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CDN, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy SCP statements for CDN.

**Table 3-88** Actions supported by CDN

| Action                       | Description                        | Access Level | Resource Type (*: required) | Condition Key                         | Alias                      |
|------------------------------|------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------|
| cdn:statistics:queryStats    | Querying domain name statistics    | list         | domain *                    | <a href="#">g:EnterpriseProjectId</a> | cdn:statistics:queryTopUrl |
| cdn:statistics:downloadExcel | Downloading domain name statistics | list         | domain *                    | <a href="#">g:EnterpriseProjectId</a> | -                          |
| cdn:log:queryLogs            | Querying logs                      | read         | domain *                    | <a href="#">g:EnterpriseProjectId</a> | -                          |

| Action                                 | Description                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                              |
|----------------------------------------|------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| cdn:charge:modifyChargeMode            | Creating or modifying the billing option | write        | -                           | -                                                                                                                                              | cdn:configuration:modifyChargeMode |
| cdn:charge:queryChargeMode             | Querying the billing option              | list         | -                           | -                                                                                                                                              | cdn:configuration:queryChargeMode  |
| cdn:statistics:querySubscriptionTasks  | Listing operations reports               | list         | -                           | -                                                                                                                                              | -                                  |
| cdn:statistics:createSubscriptionTasks | Creating an operations report            | write        | domain *                    | -                                                                                                                                              | -                                  |
| cdn:statistics:updateSubscriptionTasks | Modifying an operations report           | write        | domain *                    | -                                                                                                                                              | -                                  |
| cdn:statistics:deleteSubscriptionTasks | Deleting an operations report            | write        | -                           | -                                                                                                                                              | -                                  |
| cdn:configuration:queryDomainList      | Listing domain names                     | list         | domain *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | cdn:configuration:queryDomains     |
| cdn:configuration:queryDomains         | Querying details about a domain name     | read         | domain *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                  |
| cdn:configuration:modifyDomainConfigs  | Modifying domain name configuration      | write        | domain *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -                                  |
| cdn:configuration:modifyOriginConfInfo | Modifying the origin server settings     | write        | domain *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                  |
| cdn:log:queryLogs                      | Querying logs                            | read         | domain *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -                                  |

| Action                                   | Description                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                          |
|------------------------------------------|-----------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| cdn:statistics:queryStats                | Querying domain name statistics         | list         | domain *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | cdn:statistics:queryTopUrl     |
| cdn:configuration:queryDomainList        | Listing domain names                    | list         | domain *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | cdn:configuration:queryDomains |
| cdn:configuration:createDomains          | Creating a domain name                  | write        | domain *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | -                              |
| cdn:configuration:queryDomains           | Querying details about a domain name    | read         | domain *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| cdn:configuration:deleteDomains          | Deleting a domain name                  | write        | domain *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| cdn:configuration:disableDomains         | Disabling CDN for a domain name         | write        | domain *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| cdn:configuration:enableDomains          | Enabling CDN for a domain name          | write        | domain *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| cdn:configuration:modifyOriginServerInfo | Modifying the origin server information | write        | domain *                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |



| Action                                 | Description                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------------|--------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cdn:configuration:modifyOriginConfInfo | Modifying the origin server settings | write        | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cdn:configuration:queryOriginConfInfo  | Querying the origin server settings  | read         | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cdn:configuration:modifyReferConf      | Modifying the referer whitelist      | write        | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cdn:configuration:queryReferConf       | Querying the referer whitelist       | read         | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cdn:configuration:queryIpAcl           | Querying the IP ACL                  | list         | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cdn:configuration:modifyIpAcl          | Modifying the IP ACL                 | write        | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cdn:configuration:queryCacheRule       | Listing cache rules                  | list         | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                    | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                             |
|-------------------------------------------|--------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| cdn:configuration:modifyCacheRule         | Modifying a cache rule                     | write        | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                 |
| cdn:configuration:modifyHttpsConf         | Modifying the certificate of a domain name | write        | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                 |
| cdn:configuration:queryHttpsConf          | Querying the HTTPS settings                | read         | domain                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                 |
| cdn:configuration:queryIpInfo             | Querying the IP address information        | list         | -                           | -                                                                                                                                                  | cdn:configuration:queryDomains    |
| cdn:configuration:createResponseHeader    | Creating a response header                 | write        | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                 |
| cdn:configuration:queryResponseHeaderList | Querying response headers                  | read         | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                 |
| cdn:configuration:batchModifyHttpsConf    | Modifying certificates of domain names     | write        | domain *                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | cdn:configuration:modifyHttpsConf |
| cdn:configuration:queryTags               | Listing domain name tags                   | list         | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | cdn:configuration:queryDomains    |

| Action                                              | Description                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                                   |
|-----------------------------------------------------|-----------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| cdn:configuration:modifyTags                        | Modifying resource tags                 | tagging      | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -                                       |
| cdn:configuration:deleteTags                        | Deleting resource tags                  | tagging      | domain *                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | cdn:configuration:modifyTags            |
| cdn:configuration:refreshCache                      | Purging the cache                       | write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                           | -                                       |
| cdn:configuration:queryRefreshAndPreheatHistoryTask | Querying a cache purge or prefetch task | list         | -                           | -                                                                                                                                                                                                                                               | cdn:configuration:queryCacheHistoryTask |
| cdn:configuration:queryCacheHistoryTask             | Querying historical cache tasks         | list         | -                           | -                                                                                                                                                                                                                                               | -                                       |
| cdn:configuration:preheatCache                      | Modifying cache prefetch settings       | write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                           | -                                       |

| Action                       | Description                                                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                          |
|------------------------------|----------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------|
| cdn:configuration:queryQuota | Querying quotas of domain names, cache purge by file, cache purge by directory, and cache prefetch | list         | -                           | -             | cdn:configuration:queryDomains |

Each API of CDN usually supports one or more actions. [Table 3-89](#) lists the supported actions and dependencies.

**Table 3-89** Actions and dependencies supported by CDN APIs

| API                                                     | Action                                 | Dependencies |
|---------------------------------------------------------|----------------------------------------|--------------|
| GET /v1.0/cdn/domains                                   | cdn:configuration:queryDomainList      | -            |
| POST /v1.0/cdn/domains                                  | cdn:configuration:createDomains        | -            |
| DELETE /v1.0/cdn/domains/{domain_id}                    | cdn:configuration:deleteDomains        | -            |
| PUT /v1.0/cdn/domains/{domain_id}/disable               | cdn:configuration:disableDomains       | -            |
| PUT /v1.0/cdn/domains/{domain_id}/enable                | cdn:configuration:enableDomains        | -            |
| GET /v1.0/cdn/ip-info                                   | cdn:configuration:queryIpInfo          | -            |
| PUT /v1.0/cdn/domains/{domain_id}/private-bucket-access | cdn:configuration:modifyOriginConfInfo | -            |

| API                                                       | Action                                 | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /v1.0/cdn/domains/config-https-info                   | cdn:configuration:batchModifyHttpsConf | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| GET /v1.0/cdn/domains/https-certificate-info              | cdn:configuration:queryDomainList      | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| PUT /v1.1/cdn/configuration/domains/{domain_name}/configs | cdn:configuration:modifyOriginConfInfo | <ul style="list-style-type: none"> <li>• cdn:configuration:modifyBusinessType</li> <li>• cdn:configuration:modifyOriginServerInfo</li> <li>• cdn:configuration:modifyBackSourceUrlConfig</li> <li>• cdn:configuration:modifyHttpsConf</li> <li>• cdn:configuration:modifyCacheRule</li> <li>• cdn:configuration:modifyReferConf</li> <li>• cdn:configuration:modifyIpAcl</li> <li>• cdn:configuration:modifyUserAgent</li> <li>• cdn:configuration:modifyUrlAuth</li> <li>• cdn:configuration:createResHeader</li> <li>• cdn:configuration:modifyErrorCodeRedirectRule</li> <li>• cdn:configuration:modifyVideoSeek</li> <li>• cdn:configuration:modifyRemoteAuth</li> <li>• cdn:configuration:modifyServiceArea</li> </ul> |
| GET /v1.1/cdn/configuration/domains/{domain_name}/configs | cdn:configuration:queryDomains         | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| GET /v1.0/cdn/configuration/tags                          | cdn:configuration:queryTags            | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| POST /v1.0/cdn/configuration/tags                         | cdn:configuration:modifyTags           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| API                                                  | Action                                              | Dependencies |
|------------------------------------------------------|-----------------------------------------------------|--------------|
| POST /v1.0/cdn/configuration/tags/batch-delete       | cdn:configuration:deleteTags                        | -            |
| POST /v1.0/cdn/content/refresh-tasks                 | cdn:configuration:refreshCache                      | -            |
| POST /v1.0/cdn/content/preheating-tasks              | cdn:configuration:preheatCache                      | -            |
| GET /v1.0/cdn/historytasks                           | cdn:configuration:queryCacheHistoryTask             | -            |
| GET /v1.0/cdn/historytasks/{history_tasks_id}/detail | cdn:configuration:queryCacheHistoryTask             | -            |
| GET /v1.0/cdn/contentgateway/url-tasks               | cdn:configuration:queryRefreshAndPreheatHistoryTask | -            |
| GET /v1.0/cdn/quota                                  | cdn:configuration:queryQuota                        | -            |
| GET /v1.0/cdn/statistics/top-url                     | cdn:statistics:queryStats                           | -            |
| GET /v1.0/cdn/statistics/domain-location-stats       | cdn:statistics:queryStats                           | -            |
| GET /v1.0/cdn/statistics/domain-stats                | cdn:statistics:queryStats                           | -            |
| GET /v1.0/cdn/logs                                   | cdn:log:queryLogs                                   | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-90](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CDN.

**Table 3-90** Resource types supported by CDN

| Resource Type | URN                                    |
|---------------|----------------------------------------|
| domain        | cdn::<account-id>:domain:<domain-name> |

## Conditions

CDN does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.5.2 CloudPond

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.

- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CloudPond, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CloudPond, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CloudPond.

**Table 3-91** Actions supported by CloudPond

| Action                    | Description                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                              |
|---------------------------|-----------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------|
| ies::listServerOfferings  | Grants permission to query server offerings.  | List         | -                           | -             | <ul style="list-style-type: none"> <li>ies::system:listServerOfferings</li> </ul>  |
| ies::listNetworkOfferings | Grants permission to query network offerings. | List         | -                           | -             | <ul style="list-style-type: none"> <li>ies::system:listNetworkOfferings</li> </ul> |
| ies::listStorageTypes     | Grants permission to query storage types.     | List         | -                           | -             | <ul style="list-style-type: none"> <li>ies::system:listStorageTypes</li> </ul>     |
| ies::listSaleCycles       | Grants permission to query sale cycles.       | List         | -                           | -             | <ul style="list-style-type: none"> <li>ies::system:listSaleCycles</li> </ul>       |



| Action                                | Description                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|---------------------------------------|----------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| ies:edgeSite:listServers              | Grants permission to query servers.          | List         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| ies:edgeSite:getServer                | Grants permission to query a server.         | Read         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| ies:edgeSite:listNetworkDevices       | Grants permission to query network devices.  | List         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| ies:edgeSite:getNetworkDevice         | Grants permission to query a network device. | Read         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| ies:deliveryOrder:createDeliveryOrder | Grants permission to create delivery orders. | Write        | deliveryOrder *             | -                                     | -     |
| ies:edgeSite:create                   | Grants permission to create edge site.       | Write        | edgeSite *                  | -                                     | -     |
|                                       |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| ies:edgeSite:list                     | Grants permission to list edge sites.        | List         | edgeSite *                  | -                                     | -     |
|                                       |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| ies:edgeSite:update                   | Grants permission to update edge site.       | Write        | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| ies:edgeSite:get                      | Grants permission to view edge site details. | Read         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -     |

| Action                        | Description                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                  |
|-------------------------------|-------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------|
| ies:edgeSite:delete           | Grants permission to delete edge site.          | Write        | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                      |
| ies::listQuotas               | Grants permission to query quotas.              | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>ies:quota:list</li> </ul>       |
| ies::listRegions              | Grants permission to list regions.              | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>ies:region:list</li> </ul>      |
| ies::listZones                | Grants permission to list zones.                | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>ies:zone:list</li> </ul>        |
| ies:edgeSite:getMetricData    | Grants permission to view edge site capacity.   | Read         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | -                                                                      |
| ies:edgeSite:listRacks        | Grants permission to list racks.                | List         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ies:rack:list</li> </ul>        |
| ies:edgeSite:getRack          | Grants permission to view rack details.         | Read         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ies:rack:get</li> </ul>         |
| ies:edgeSite:listStoragePools | Grants permission to list storage pools.        | List         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ies:storagePool:list</li> </ul> |
| ies:edgeSite:getStoragePool   | Grants permission to view storage pool details. | Read         | edgeSite *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ies:storagePool:get</li> </ul>  |

Each API of CloudPond usually supports one or more actions. [Table 3-92](#) lists the supported actions and dependencies.

**Table 3-92** Actions and dependencies supported by CloudPond APIs

| API                                                     | Action                          | Dependencies |
|---------------------------------------------------------|---------------------------------|--------------|
| GET /v2/{domain_id}/server-offerings                    | ies::listServerOfferings        | -            |
| GET /v2/{domain_id}/network-device-offerings            | ies::listNetworkOfferings       | -            |
| GET /v2/{domain_id}/storage-types                       | ies::listStorageTypes           | -            |
| GET /v2/{domain_id}/sale-cycles                         | ies::listSaleCycles             | -            |
| GET /v2/{domain_id}/servers                             | ies:edgeSite:listServers        | -            |
| GET /v2/{domain_id}/servers/{server_id}                 | ies:edgeSite:getServer          | -            |
| GET /v2/{domain_id}/network-devices                     | ies:edgeSite:listNetworkDevices | -            |
| GET /v2/{domain_id}/network-devices/{network_device_id} | ies:edgeSite:getNetworkDevice   | -            |
| GET /v2/{domain_id}/storage-pools                       | ies:edgeSite:listStoragePools   | -            |
| GET /v2/{domain_id}/storage-pools/{id}                  | ies:edgeSite:getStoragePool     | -            |
| GET /v2/{domain_id}/storage-gears                       | ies::listSupportedStorageGears  | -            |
| POST /v1/{domain_id}/edge-sites                         | ies:edgeSite:create             | -            |
| GET /v1/{domain_id}/edge-sites                          | ies:edgeSite:list               | -            |

| API                                                  | Action                     | Dependencies |
|------------------------------------------------------|----------------------------|--------------|
| PUT /v1/{domain_id}/edge-sites/{site_id}             | ies:edgeSite:update        | -            |
| GET /v1/{domain_id}/edge-sites/{site_id}             | ies:edgeSite:get           | -            |
| DELETE /v1/{domain_id}/edge-sites/{site_id}          | ies:edgeSite:delete        | -            |
| GET /v1/{domain_id}/quotas                           | ies::listQuotas            | -            |
| GET /v1/{domain_id}/regions                          | ies::listRegions           | -            |
| GET /v1/{domain_id}/zones                            | ies::listZones             | -            |
| GET /v1/{domain_id}/edge-sites/{site_id}/metric-data | ies:edgeSite:getMetricData | -            |
| GET /v1/{domain_id}/racks                            | ies:edgeSite:listRacks     | -            |
| GET /v1/{domain_id}/racks/{id}                       | ies:edgeSite:getRack       | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-93](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CloudPond.

**Table 3-93** Resource types supported by CloudPond

| Resource Type | URN                                 |
|---------------|-------------------------------------|
| edgeSite      | ies::<domain-id>:edgeSite:<site-id> |

| Resource Type | URN                                                |
|---------------|----------------------------------------------------|
| deliveryOrder | ies::<domain-id>:deliveryOrder:<delivery-order-id> |

## Conditions

CloudPond does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.6 Databases

### 3.6.1 Relational Database Service (RDS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [service control policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.

- If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by RDS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by RDS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for RDS.

**Table 3-94** Actions supported by RDS

| Action                       | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias                |
|------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|----------------------|
| rds:param:apply              | Grants permission to apply a parameter template.                       | write        | -                           | -                                                                                      | -                    |
| rds:instance:updateParameter | Grants permission to modify parameters of an instance.                 | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:parameter:modify |
| rds:instance:restoreInPlace  | Grants permission to restore data to an existing or original instance. | write        | -                           | -                                                                                      | -                    |

| Action                           | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias        |
|----------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|--------------|
| rds:instance:tableRestore        | Grants permission to restore tables.                                            | write        | -                           | -                                                                                      | -            |
| rds:database:drop                | Grants permission to delete a database.                                         | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -            |
| rds:log:getSlowLogs              | Grants permission to query slow query log statistics.                           | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:list |
| rds:instance:listDatabaseVersion | Grants permission to query the database version information.                    | read         | -                           | -                                                                                      | -            |
| rds:instance:listFlavors         | Grants permission to query specifications.                                      | read         | -                           | -                                                                                      | -            |
| rds:instance:listStorageType     | Grants permission to query storage types.                                       | read         | -                           | -                                                                                      | -            |
| rds:instance:create              | Grants permission to create a DB instance or restore data to a new DB instance. | write        | -                           | -                                                                                      | -            |

| Action                     | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias                      |
|----------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|----------------------------|
| rds:instance:stop          | Grants permission to stop an instance.               | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:operateServer |
| rds:instance:start         | Grants permission to start an instance.              | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:operateServer |
| rds:instance:updateName    | Grants permission to change an instance name.        | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modify        |
| rds:instance:updateRemark  | Grants permission to modify an instance description. | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modify        |
| rds:instance:createDns     | Grants permission to create a private DNS server.    | write        | -                           | -                                                                                      | -                          |
| rds:instance:updateDnsName | Grants permission to modify a domain name.           | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modifyDns     |



| Action                            | Description                                                       | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias                  |
|-----------------------------------|-------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|------------------------|
| rds:instance:getDnsName           | Grants permission to query the domain name of an instance.        | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list      |
| rds:instance:getDnsName           | Grants permission to query the IPv6 domain name of an instance.   | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list      |
| rds:instance:getReplicaStatus     | Grants permission to query the replication status of an instance. | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list      |
| rds:instance:modifySpec           | Grants permission to change instance specifications.              | write                 | -                           | -                                                                                      | -                      |
| rds:instance:extendSpace          | Grants permission to scale up storage space of an instance.       | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                      |
| rds:instance:setAutoEnlargePolicy | Grants permission to configure a storage autoscaling policy.      | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modifyDns |

| Action                            | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|-----------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:instance:getAutoEnlargePolicy | Grants permission to query an autoscaling policy.                            | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list   |
| rds:instance:singleToHa           | Grants permission to change an instance from single-node to primary/standby. | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:instance:restart              | Grants permission to reboot an instance.                                     | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:instance:deleteInstance       | Grants permission to delete a DB instance.                                   | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:delete |
| rds:instance:listAll              | Grants permission to query DB instances.                                     | read         | -                           | -                                                                                      | rds:instance:list   |
| rds:instance:modifyPublicAccess   | Grants permission to bind and unbind an EIP.                                 | write        | -                           | -                                                                                      | -                   |

| Action                             | Description                                                                         | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias |
|------------------------------------|-------------------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|-------|
| rds:instance:modifyStrategy        | Grants permission to configure the failover priority of a primary/standby instance. | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:instance:switchover            | Grants permission to perform a primary/standby switchover.                          | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:instance:modifySyncronizeModel | Grants permission to configure the replication mode of a primary/standby instance.  | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:instance:openReadonly          | Grants permission to set an instance to read-only.                                  | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:instance:create                | Grants permission to migrate a standby instance.                                    | write                 | -                           | -                                                                                      | -     |

| Action                                      | Description                                                            | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|---------------------------------------------|------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:instance:updateOpsWindow                | Grants permission to configure the maintenance window of an instance.  | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modify |
| rds:instance:upgradeDatabaseVersion         | Grants permission to upgrade the version of an instance.               | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modify |
| rds:instance:enableSecondLevelMonitoring    | Grants permission to enable Monitoring by Seconds.                     | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:switch      |
| rds:instance:getSecondLevelMonitoringConfig | Grants permission to query the configuration of Monitoring by Seconds. | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:list        |

| Action                        | Description                                                                                                       | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|-------------------|
| rds:instance:buildDrRelation  | Grants permission to configure DR capabilities for primary and DR instances, and promote DR instances to primary. | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:instance:getReplicaStatus | Grants permission to query the DR replication status.                                                             | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list |
| rds:instance:listAll          | Grants permission to query DR instances in batches.                                                               | read                  | -                           | -                                                                                      | rds:instance:list |
| rds:instance:modifySSL        | Grants permission to enable or disable SSL.                                                                       | permission_management | -                           | -                                                                                      | -                 |
| rds:instance:modifySSL        | Grants permission to obtain the SSL certificate download address.                                                 | permission_management | -                           | -                                                                                      | -                 |

| Action                           | Description                                                            | Access Level          | Resource Type (*: required) | Condition Key                                                                                                               | Alias             |
|----------------------------------|------------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------|
| rds:instance:modifyPort          | Grants permission to change a database port.                           | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                      | -                 |
| rds:instance:modifySecurityGroup | Grants permission to modify a security group.                          | write                 | -                           | -                                                                                                                           | -                 |
| rds:instance:modifyIp            | Grants permission to change a floating IP address.                     | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                      | -                 |
| rds:instance:modifyBackupPolicy  | Grants permission to configure an automated backup policy.             | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">rds:BackupEnabled</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:instance:modifyBackupPolicy  | Grants permission to configure a cross-region automated backup policy. | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">rds:BackupEnabled</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:instance:getBackupPolicy     | Grants permission to query an automated backup policy.                 | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                      | rds:instance:list |

| Action                       | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias             |
|------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|-------------------|
| rds:instance:getBackupPolicy | Grants permission to query a cross-region automated backup policy.                  | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list |
| rds:backup:create            | Grants permission to create a manual backup.                                        | write        | -                           | -                                                                                      | -                 |
| rds:backup:list              | Grants permission to query backups.                                                 | list         | -                           | -                                                                                      | -                 |
| rds:backup:list              | Grants permission to query cross-region backups.                                    | list         | -                           | -                                                                                      | -                 |
| rds:instance:listAll         | Grants permission to query DB instances for which cross-region backups are created. | read         | -                           | -                                                                                      | rds:instance:list |
| rds:backup:download          | Grants permission to obtain a backup download link.                                 | read         | -                           | -                                                                                      | -                 |

| Action                      | Description                                                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|-------------------|
| rds:backup:delete           | Grants permission to delete a manual backup.                                                                        | write        | -                           | -                                                                                      | -                 |
| rds:instance:getRestoreTime | Grants permission to query the restoration time range of an instance.                                               | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list |
| rds:instance:getRestoreTime | Grants permission to query the restoration time range of a cross-region backup.                                     | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list |
| rds:instance:tableRestore   | Grants permission to check whether fast restoration can be used for restoring databases or tables of a DB instance. | write        | -                           | -                                                                                      | -                 |



| Action                    | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key | Alias             |
|---------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------|
| rds:backup:list           | Grants permission to query databases that can be restored to a specified point in time. | list         | -                           | -             | -                 |
| rds:instance:tableRestore | Grants permission to restore databases to a point in time.                              | write        | -                           | -             | -                 |
| rds:instance:listAll      | Grants permission to query the target version to which a DB instance can be upgraded.   | read         | -                           | -             | rds:instance:list |
| rds:instance:listAll      | Grants permission to perform a major version upgrade pre-check for a DB instance.       | read         | -                           | -             | rds:instance:list |

| Action               | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|----------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:instance:listAll | Grants permission to query the major version check status or upgrade status of a DB instance | read         | -                           | -                                                                                      | rds:instance:list   |
| rds:instance:listAll | Grants permission to query the major version upgrade check history of a DB instance.         | read         | -                           | -                                                                                      | rds:instance:list   |
| rds:instance:update  | Grants permission to upgrade a major version.                                                | read         | -                           | -                                                                                      | rds:instance:modify |
| rds:instance:listAll | Grants permission to query the major version upgrade history of a DB instance.               | read         | -                           | -                                                                                      | rds:instance:list   |
| rds:log:getSlowLogs  | Grants permission to query slow query logs.                                                  | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:list        |

| Action                            | Description                                                      | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias          |
|-----------------------------------|------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|----------------|
| rds:log:getErrorLogs              | Grants permission to query database error logs.                  | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:list   |
| rds:log:setSlowLogSensitiveStatus | Grants permission to show original slow query logs.              | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:switch |
| rds:log:getSlowLogs               | Grants permission to query slow query log files.                 | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:list   |
| rds:log:getErrorLogs              | Grants permission to query extended logs.                        | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:log:list   |
| rds:log:download                  | Grants permission to obtain links for downloading extended logs. | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -              |
| rds:log:download                  | Grants permission to download slow query logs.                   | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -              |
| rds:auditlog:operate              | Grants permission to configure an audit log policy.              | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -              |

| Action                | Description                                                          | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias             |
|-----------------------|----------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|-------------------|
| rds:auditlog:list     | Grants permission to query the policy for audit logs.                | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:auditlog:list     | Grants permission to query audit logs.                               | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:auditlog:download | Grants permission to obtain the link for downloading audit logs.     | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:binlog:setPolicy  | Grants permission to configure a binlog policy.                      | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:binlog:get        | Grants permission to query binlogs.                                  | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                 |
| rds:instance:listAll  | Grants permission to obtain the number of instances after diagnosis. | read                  | -                           | -                                                                                      | rds:instance:list |
| rds:instance:listAll  | Grants permission to obtain the result of a specific diagnosis item. | read                  | -                           | -                                                                                      | rds:instance:list |

| Action                       | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:instance:modifyProxy     | Grants permission to enable or disable database proxy.                | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:instance:getDBProxy      | Grants permission to query information about a database proxy.        | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list   |
| rds:instance:getProxyFlavors | Grants permission to query database proxy specifications.             | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list   |
| rds:instance:modifyProxy     | Grants permission to configure a routing policy for a database proxy. | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:database:createDatabase  | Grants permission to create a database.                               | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:database:create |
| rds:database:list            | Grants permission to query databases.                                 | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |

| Action                  | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|-------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:database:update     | Grants permission to modify the database remarks of a DB instance.   | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:database:create |
| rds:database:drop       | Grants permission to delete a database.                              | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:create | Grants permission to create a database account.                      | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:list   | Grants permission to query database users.                           | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:list   | Grants permission to query authorized users of a specified database. | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:update | Grants permission to modify the remarks of a database account.       | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:drop   | Grants permission to delete a database account.                      | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |

| Action                       | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:password:update          | Grants permission to change a database password.               | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databasePrivilege:grant  | Grants permission to authorize a database account.             | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databasePrivilege:revoke | Grants permission to revoke permissions of a database account. | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:password:update          | Grants permission to reset the password for user root.         | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:database:createDatabase  | Grants permission to create a database.                        | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:database:create |
| rds:databaseUser:create      | Grants permission to create a database account.                | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:database:update          | Grants permission to create a database schema.                 | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:database:create |

| Action                      | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias |
|-----------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|-------|
| rds:databasePrivilege:grant | Grants permission to grant read or write permissions to a database account. | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:databasePrivilege:grant | Grants permission to grant operation permissions to a database account.     | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:password:update         | Grants permission to change a database password.                            | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:database:list           | Grants permission to query databases.                                       | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:databaseUser:list       | Grants permission to query database users.                                  | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:database:list           | Grants permission to query database schemas.                                | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:databasePrivilege:grant | Grants permission to configure account permissions.                         | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |



| Action                  | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|-------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:database:update     | Grants permission to modify the database remarks of a DB instance.               | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:database:create |
| rds:databaseUser:update | Grants permission to modify the remarks of a database account.                   | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:database:drop       | Grants permission to delete a database.                                          | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:drop   | Grants permission to delete a database account.                                  | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:list   | Grants permission to query the pg_hba.conf file configurations of a DB instance. | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:databaseUser:update | Grants permission to modify or add one or more records in the pg_hba.conf file.  | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |

| Action                       | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias                |
|------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|----------------------|
| rds:database User:create     | Grants permission to overwrite the pg_hba.conf file.                        | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                    |
| rds:database User:drop       | Grants permission to delete one or more records from the pg_hba.conf file.  | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                    |
| rds:database User:list       | Grants permission to query the pg_hba.conf change history of a DB instance. | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                    |
| rds:database: list           | Grants permission to query available SQL Server character sets.             | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                    |
| rds:database: createDatabase | Grants permission to create a database.                                     | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds: database:create |
| rds:database: list           | Grants permission to query databases.                                       | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                    |

| Action                        | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias |
|-------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|-------|
| rds:database User:create      | Grants permission to create a database account.                      | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:password:update           | Grants permission to change a database password.                     | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:database User:list        | Grants permission to query database users.                           | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:database User:list        | Grants permission to query authorized users of a specified database. | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:database User:drop        | Grants permission to delete a database account.                      | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:database Privilege:grant  | Grants permission to authorize a database account.                   | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| rds:database Privilege:revoke | Grants permission to revoke permissions of a database account.       | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                               | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|--------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:instance:SetMsdtcHosts           | Grants permission to add MSDTC hosts.                             | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modify |
| rds:instance:getMsdtcHosts           | Grants permission to query MSDTC hosts.                           | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list   |
| rds:param:listAll                    | Grants permission to query parameter templates.                   | list         | -                           | -                                                                                      | rds:param:list      |
| rds:param:createTemplate             | Grants permission to create a parameter template.                 | write        | -                           | -                                                                                      | rds:param:create    |
| rds:param:updateTemplate             | Grants permission to modify parameters in a parameter template.   | write        | -                           | -                                                                                      | rds:param:modify    |
| rds:param:copy                       | Grants permission to replicate a parameter template.              | write        | -                           | -                                                                                      | rds:param:create    |
| rds:param:listInstanceParamHistories | Grants permission to query change history of instance parameters. | list         | -                           | -                                                                                      | rds:param:list      |

| Action                    | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias                |
|---------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|----------------------|
| rds:instance:getParameter | Grants permission to query the parameter template of an instance. | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:parameter: list  |
| rds:param:get             | Grants permission to query parameters of a parameter template.    | read         | -                           | -                                                                                      | rds:parameter: list  |
| rds:param:get             | Grants permission to delete a parameter template.                 | read         | -                           | -                                                                                      | -                    |
| rds:database:update       | Grants permission to create an extension.                         | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:database: create |
| rds:database: list        | Grants permission to query extensions.                            | list         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                    |
| rds:database: drop        | Grants permission to delete an extension.                         | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                    |

| Action                       | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias                |
|------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|----------------------|
| rds:instance:updateParameter | Grants permission to modify the value of a specified parameter for a DB instance. | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:parameter:modify |
| rds:instance:getParameter    | Grants permission to obtain the value of a specified parameter for a DB instance. | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:parameter:list   |
| rds:instance:setRecycleBin   | Grants permission to configure a recycling policy.                                | write        | -                           | -                                                                                      | -                    |
| rds:instance:listAll         | Grants permission to query the recycling policy.                                  | read         | -                           | -                                                                                      | rds:instance:list    |
| rds:instance:listAll         | Grants permission to query DB instances in the recycle bin.                       | read         | -                           | -                                                                                      | rds:instance:list    |
| rds:instance:createTag       | Grants permission to add tags in batches.                                         | write        | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:dealTag |

| Action                  | Description                                                                                        | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias                  |
|-------------------------|----------------------------------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|------------------------|
| rds:instance:deleteTag  | Grants permission to delete tags in batches.                                                       | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:deleteTag |
| rds:tag:list            | Grants permission to query project tags.                                                           | list                  | -                           | -                                                                                      | -                      |
| rds:instance:listQuotas | Grants permission to query resource quotas.                                                        | read                  | -                           | -                                                                                      | rds:instance:list      |
| rds:task:listAll        | Grants permission to obtain task information.                                                      | list                  | -                           | -                                                                                      | rds:task:list          |
| rds:task:listAll        | Grants permission to obtain task information of a specified DB instance in a specified time range. | list                  | -                           | -                                                                                      | rds:task:list          |
| rds:instance:toggleTDE  | Grants permission to enable TDE.                                                                   | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                      |

| Action                               | Description                                                      | Access Level          | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|--------------------------------------|------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:instance:deleteDisasterRecovery  | Grants permission to remove a DR relationship.                   | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:instance:showReplayDelayStatus   | Grants permission to query the log replay delay status.          | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list   |
| rds:instance:switchLogReplay         | Grants permission to stop and resume log replay.                 | write                 | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:modify |
| rds:instance:queryRecoveryTimeWindow | Grants permission to query the recovery time window of WAL logs. | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list   |
| rds:binlog:setPolicy                 | Grants permission to set the retention period for local binlogs. | permission_management | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |
| rds:binlog:get                       | Grants permission to get the retention period for local binlogs. | read                  | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                   |



| Action               | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                          | Alias               |
|----------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------|---------------------|
| rds:instance:listAll | Grants permission to obtain the number of instances after diagnosis. | read         | -                           | -                                                                                      | rds:instance:list   |
| rds:instance:listAll | Grants permission to obtain the result of a specific diagnosis item. | read         | -                           | -                                                                                      | rds:instance:list   |
| rds:instance:update  | Grants permission to add SQL throttling rules.                       | read         | -                           | -                                                                                      | rds:instance:modify |
| rds:instance:update  | Grants permission to delete SQL throttling rules.                    | read         | -                           | -                                                                                      | rds:instance:modify |
| rds:instance:update  | Grants permission to modify SQL throttling rules.                    | read         | -                           | -                                                                                      | rds:instance:modify |
| rds:instance:get     | Grants permission to query SQL throttling rules.                     | read         | instance                    | <a href="#">g:EnterpriseProjectId</a><br><a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | rds:instance:list   |

| Action              | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias               |
|---------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------|
| rds:instance:update | Grants permission to enable or disable a SQL throttling rule or disable all SQL throttling rules. | read         | -                           | -             | rds:instance:modify |
| rds:instance:update | Grants permission to unlock an instance from the read-only state.                                 | read         | -                           | -             | rds:instance:modify |

Each API of RDS usually supports one or more actions. [Table 3-95](#) lists the supported actions and dependencies.

**Table 3-95** Actions and dependencies supported by RDS APIs

| API                                                                  | Action                           | Dependencies |
|----------------------------------------------------------------------|----------------------------------|--------------|
| PUT /v3.1/{project_id}/configurations/{config_id}/apply              | rds:param:apply                  | -            |
| PUT /v3.1/{project_id}/instances/{instance_id}/configurations        | rds:instance:update Parameter    | -            |
| POST /v3.1/{project_id}/instances/recovery                           | rds:instance:restore InPlace     | -            |
| POST /v3.1/{project_id}/instances/{instance_id}/restore/tables       | rds:instance:tableRestore        | -            |
| DELETE /v3.1/{project_id}/instances/{instance_id}/database/{db_name} | rds:database:drop                | -            |
| POST /v3.1/{project_id}/instances/{instance_id}/slow-logs/statistics | rds:log:getSlowLogs              | -            |
| GET /v3/{project_id}/datastores/{database_name}                      | rds:instance:listDatabaseVersion | -            |

| API                                                                                                                          | Action                            | Dependencies |
|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|--------------|
| GET /v3/{project_id}/flavors/{database_name}?version_name={version_name}&spec_code={spec_code}&is_serverless={is_serverless} | rds:instance:listFlavors          | -            |
| GET /v3/{project_id}/storage-type/{database_name}?version_name={version_name}&ha_mode={ha_mode}                              | rds:instance:listStorageType      | -            |
| POST /v3/{project_id}/instances                                                                                              | rds:instance:create               | -            |
| POST /v3/{project_id}/instances/{instance_id}/action/shutdown                                                                | rds:instance:stop                 | -            |
| POST /v3/{project_id}/instances/{instance_id}/action/startup                                                                 | rds:instance:start                | -            |
| PUT /v3/{project_id}/instances/{instance_id}/name                                                                            | rds:instance:updateName           | -            |
| PUT /v3/{project_id}/instances/{instance_id}/alias                                                                           | rds:instance:updateRemark         | -            |
| POST /v3/{project_id}/instances/{instance_id}/create-dns                                                                     | rds:instance:createDns            | -            |
| PUT /v3/{project_id}/instances/{instance_id}/modify-dns                                                                      | rds:instance:updateDnsName        | -            |
| GET /v3/{project_id}/instances/{instance_id}/dns                                                                             | rds:instance:getDnsName           | -            |
| GET /v3/{project_id}/instances/{instance_id}/dns-ipv6                                                                        | rds:instance:getDnsName           | -            |
| GET /v3/{project_id}/instances/{instance_id}/replication/status                                                              | rds:instance:getReplicaStatus     | -            |
| POST /v3/{project_id}/instances/{instance_id}/action                                                                         | rds:instance:modifySpec           | -            |
| POST /v3/{project_id}/instances/{instance_id}/action                                                                         | rds:instance:extendSpace          | -            |
| PUT /v3/{project_id}/instances/{instance_id}/disk-auto-expansion                                                             | rds:instance:setAutoEnlargePolicy | -            |
| GET /v3/{project_id}/instances/{instance_id}/disk-auto-expansion                                                             | rds:instance:getAutoEnlargePolicy | -            |
| POST /v3/{project_id}/instances/{instance_id}/action                                                                         | rds:instance:singleToHa           | -            |

| API                                                                 | Action                                      | Dependencies |
|---------------------------------------------------------------------|---------------------------------------------|--------------|
| POST /v3/{project_id}/instances/{instance_id}/action                | rds:instance:restart                        | -            |
| DELETE /v3/{project_id}/instances/{instance_id}                     | rds:instance:deleteInstance                 | -            |
| GET /v3/{project_id}/instances                                      | rds:instance:listAll                        | -            |
| PUT /v3/{project_id}/instances/{instance_id}/public-ip              | rds:instance:modifyPublicAccess             | -            |
| PUT /v3/{project_id}/instances/{instance_id}/failover/strategy      | rds:instance:modifyStrategy                 | -            |
| PUT /v3/{project_id}/instances/{instance_id}/failover               | rds:instance:switchover                     | -            |
| PUT /v3/{project_id}/instances/{instance_id}/failover/mode          | rds:instance:modifySynchronizeModel         | -            |
| PUT /v3/{project_id}/instances/{instance_id}/readonly-status        | rds:instance:openReadOnly                   | -            |
| POST /v3/{project_id}/instances/{instance_id}/migrateslave          | rds:instance:create                         | -            |
| PUT /v3/{project_id}/instances/{instance_id}/ops-window             | rds:instance:updateOpsWindow                | -            |
| POST /v3/{project_id}/instances/{instance_id}/db-upgrade            | rds:instance:upgradeDatabaseVersion         | -            |
| PUT /v3/{project_id}/instances/{instance_id}/second-level-monitor   | rds:instance:enableSecondLevelMonitoring    | -            |
| GET /v3/{project_id}/instances/{instance_id}/second-level-monitor   | rds:instance:getSecondLevelMonitoringConfig | -            |
| POST /v3/{project_id}/instances/{instance_id}/action                | rds:instance:buildDRRelation                | -            |
| GET /v3/{project_id}/instances/{instance_id}/disaster-recovery      | rds:instance:getReplicaStatus               | -            |
| GET /v3/{project_id}/instances/disaster-recovery-relation           | rds:instance:listAll                        | -            |
| PUT /v3/{project_id}/instances/{instance_id}/ssl                    | rds:instance:modifySSL                      | -            |
| GET /v3/{project_id}/instances/{instance_id}/ssl-cert/download-link | rds:instance:modifySSL                      | -            |

| API                                                                                                                                                                                      | Action                           | Dependencies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|--------------|
| PUT /v3/{project_id}/instances/{instance_id}/port                                                                                                                                        | rds:instance:modifyPort          | -            |
| PUT /v3/{project_id}/instances/{instance_id}/security-group                                                                                                                              | rds:instance:modifySecurityGroup | -            |
| PUT /v3/{project_id}/instances/{instance_id}/ip                                                                                                                                          | rds:instance:modifyIp            | -            |
| PUT /v3/{project_id}/instances/{instance_id}/backups/policy                                                                                                                              | rds:instance:modifyBackupPolicy  | -            |
| PUT /v3/{project_id}/instances/{instance_id}/backups/offsite-policy                                                                                                                      | rds:instance:modifyBackupPolicy  | -            |
| GET /v3/{project_id}/instances/{instance_id}/backups/policy                                                                                                                              | rds:instance:getBackupPolicy     | -            |
| GET /v3/{project_id}/instances/{instance_id}/backups/offsite-policy                                                                                                                      | rds:instance:getBackupPolicy     | -            |
| POST /v3/{project_id}/backups                                                                                                                                                            | rds:backup:create                | -            |
| GET /v3/{project_id}/backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin_time}&end_time={end_time}         | rds:backup:list                  | -            |
| GET /v3/{project_id}/offsite-backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin_time}&end_time={end_time} | rds:backup:list                  | -            |
| GET /v3/backups/offsite-backup-instance?offset={offset}&limit={limit}                                                                                                                    | rds:instance:listAll             | -            |
| GET /v3/{project_id}/backup-files?backup_id={backup_id}                                                                                                                                  | rds:backup:download              | -            |
| DELETE /v3/{project_id}/backups/{backup_id}                                                                                                                                              | rds:backup:delete                | -            |
| GET /v3/{project_id}/instances/{instance_id}/restore-time?date=2020-12-26                                                                                                                | rds:instance:getRestoreTime      | -            |
| GET /v3/{project_id}/instances/{instance_id}/offsite-restore-time?date=2020-12-26                                                                                                        | rds:instance:getRestoreTime      | -            |

| API                                                                                                                                                                                                             | Action                            | Dependencies |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|--------------|
| POST /v3/{project_id}/instances/fast-restore                                                                                                                                                                    | rds:instance:tableRestore         | -            |
| POST /v3/{project_id}/{engine}/instances/history/databases                                                                                                                                                      | rds:backup:list                   | -            |
| POST /v3/{project_id}/instances/batch/restore/databases                                                                                                                                                         | rds:instance:tableRestore         | -            |
| GET /v3/{project_id}/instances/{instance_id}/major-version/available-version                                                                                                                                    | rds:instance:listAll              | -            |
| POST /v3/{project_id}/instances/{instance_id}/major-version/inspection                                                                                                                                          | rds:instance:listAll              | -            |
| GET /v3/{project_id}/instances/{instance_id}/major-version/status?action={current_action}                                                                                                                       | rds:instance:listAll              | -            |
| GET /v3/{project_id}/instances/{instance_id}/major-version/inspection-histories?offset={offset}&limit={limit}&order={order}&sort_field={sort_field}&target_version={target_version}&is_available={is_available} | rds:instance:listAll              | -            |
| POST /v3/{project_id}/instances/{instance_id}/major-version/upgrade                                                                                                                                             | rds:instance:update               | -            |
| GET /v3/{project_id}/instances/{instance_id}/major-version/upgrade-histories?offset={offset}&limit={limit}&order={order}&sort_field={sort_field}                                                                | rds:instance:listAll              | -            |
| POST /v3/{project_id}/instances/{instance_id}/slow-logs                                                                                                                                                         | rds:log:getSlowLogs               | -            |
| POST /v3/{project_id}/instances/{instance_id}/error-logs                                                                                                                                                        | rds:log:getErrorLogs              | -            |
| PUT /v3/{project_id}/instances/{instance_id}/slowlog-sensitization/{status}                                                                                                                                     | rds:log:setSlowLogSensitiveStatus | -            |
| GET /v3/{project_id}/instances/{instance_id}/slowlog-files                                                                                                                                                      | rds:log:getSlowLogs               | -            |
| GET /v3/{project_id}/instances/{instance_id}/xelog-files                                                                                                                                                        | rds:log:getErrorLogs              | -            |
| POST /v3/{project_id}/instances/{instance_id}/xelog-download                                                                                                                                                    | rds:log:download                  | -            |

| API                                                                                                                             | Action                       | Dependencies |
|---------------------------------------------------------------------------------------------------------------------------------|------------------------------|--------------|
| POST /v3/{project_id}/instances/{instance_id}/slowlog-download                                                                  | rds:log:download             | -            |
| PUT /v3/{project_id}/instances/{instance_id}/auditlog-policy                                                                    | rds:auditlog:operate         | -            |
| GET /v3/{project_id}/instances/{instance_id}/auditlog-policy                                                                    | rds:auditlog:list            | -            |
| GET /v3/{project_id}/instances/{instance_id}/auditlog?start_time={start_time}&end_time={end_time}&offset={offset}&limit={limit} | rds:auditlog:list            | -            |
| POST /v3/{project_id}/instances/{instance_id}/auditlog-links                                                                    | rds:auditlog:download        | -            |
| PUT /v3/{project_id}/instances/{instance_id}/binlog/clear-policy                                                                | rds:binlog:setPolicy         | -            |
| GET /v3/{project_id}/instances/{instance_id}/binlog/clear-policy                                                                | rds:binlog:get               | -            |
| GET /v3/{project_id}/instances/diagnosis                                                                                        | rds:instance:listAll         | -            |
| GET /v3/{project_id}/instances/diagnosis/info                                                                                   | rds:instance:listAll         | -            |
| POST /v3/{project_id}/instances/{instance_id}/proxy/open                                                                        | rds:instance:modifyProxy     | -            |
| GET /v3/{project_id}/instances/{instance_id}/proxy-list                                                                         | rds:instance:getDBProxy      | -            |
| GET /v3/{project_id}/instances/{instance_id}/proxy/flavors                                                                      | rds:instance:getProxyFlavors | -            |
| POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/route-mode                                                       | rds:instance:modifyProxy     | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}                                                                | rds:instance:modifyProxy     | -            |
| POST /v3/{project_id}/instances/{instance_id}/database                                                                          | rds:database:createDatabase  | -            |
| GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}                                          | rds:database:list            | -            |
| POST /v3/{project_id}/instances/{instance_id}/database/update                                                                   | rds:database:update          | -            |

| API                                                                                                       | Action                       | Dependencies |
|-----------------------------------------------------------------------------------------------------------|------------------------------|--------------|
| DELETE /v3/{project_id}/instances/{instance_id}/database/{db_name}                                        | rds:database:drop            | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_user                                                     | rds:databaseUser:create      | -            |
| GET /v3/{project_id}/instances/{instance_id}/db_user/detail?page={page}&limit={limit}                     | rds:databaseUser:list        | -            |
| GET /v3/{project_id}/instances/{instance_id}/database/db_user?db-name={db-name}&page={page}&limit={limit} | rds:databaseUser:list        | -            |
| PUT /v3/{project_id}/instances/{instance_id}/db-users/{user_name}/comment                                 | rds:databaseUser:update      | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db_user/{user_name}                                       | rds:databaseUser:drop        | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_user/resetpwd                                            | rds:password:update          | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_privilege                                                | rds:databasePrivilege:grant  | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db_privilege                                              | rds:databasePrivilege:revoke | -            |
| POST /v3/{project_id}/instances/{instance_id}/password                                                    | rds:password:update          | -            |
| POST /v3/{project_id}/instances/{instance_id}/database                                                    | rds:database:create Database | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_user                                                     | rds:databaseUser:create      | -            |
| POST /v3/{project_id}/instances/{instance_id}/schema                                                      | rds:database:update          | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_privilege                                                | rds:databasePrivilege:grant  | -            |
| POST /v3/{project_id}/instances/{instance_id}/db-user-privilege                                           | rds:databasePrivilege:grant  | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_user/resetpwd                                            | rds:password:update          | -            |
| GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}                    | rds:database:list            | -            |



| API                                                                                                                                    | Action                       | Dependencies |
|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------|--------------|
| GET /v3/{project_id}/instances/{instance_id}/db_user/detail?page={page}&limit={limit}                                                  | rds:databaseUser:list        | -            |
| GET /v3/{project_id}/instances/{instance_id}/schema/detail?db_name={name}&page={page}&limit={limit}                                    | rds:database:list            | -            |
| POST /v3/{project_id}/instances/{instance_id}/user-privilege                                                                           | rds:databasePrivilege:grant  | -            |
| POST /v3/{project_id}/instances/{instance_id}/database/update                                                                          | rds:database:update          | -            |
| PUT /v3/{project_id}/instances/{instance_id}/db-users/{user_name}/comment                                                              | rds:databaseUser:update      | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/database/{db_name}                                                                     | rds:database:drop            | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db_user/{user_name}                                                                    | rds:databaseUser:drop        | -            |
| GET /v3/{project_id}/instances/{instance_id}/hba-info                                                                                  | rds:databaseUser:list        | -            |
| PUT /v3/{project_id}/instances/{instance_id}/hba-info                                                                                  | rds:databaseUser:update      | -            |
| POST /v3/{project_id}/instances/{instance_id}/hba-info                                                                                 | rds:databaseUser:create      | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/hba-info                                                                               | rds:databaseUser:drop        | -            |
| GET /v3/{project_id}/instances/{instance_id}/hba-info/history                                                                          | rds:databaseUser:list        | -            |
| GET /v3/{project_id}/collations                                                                                                        | rds:database:list            | -            |
| POST /v3/{project_id}/instances/{instance_id}/database                                                                                 | rds:database:create Database | -            |
| GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}&db-name={db-name}&recover_model={recover_model} | rds:database:list            | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_user                                                                                  | rds:databaseUser:create      | -            |

| API                                                                                                                                                                    | Action                               | Dependencies |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| POST /v3/{project_id}/instances/{instance_id}/db_user/resetpwd                                                                                                         | rds:password:update                  | -            |
| GET /v3/{project_id}/instances/{instance_id}/db_user/detail?page={page}&limit={limit}                                                                                  | rds:databaseUser:list                | -            |
| GET /v3/{project_id}/instances/{instance_id}/database/db_user?db-name={db-name}&page={page}&limit={limit}                                                              | rds:databaseUser:list                | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db_user/{user_name}                                                                                                    | rds:databaseUser:drop                | -            |
| POST /v3/{project_id}/instances/{instance_id}/db_privilege                                                                                                             | rds:databasePrivilege:grant          | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db_privilege                                                                                                           | rds:databasePrivilege:revoke         | -            |
| POST /v3/{project_id}/instances/{instance_id}/msdtc/host                                                                                                               | rds:instance:SetMsdtcHosts           | -            |
| GET /v3/{project_id}/instances/{instance_id}/msdtc/hosts?offset={offset}&limit={limit}                                                                                 | rds:instance:getMsdtcHosts           | -            |
| GET /v3/{project_id}/configurations                                                                                                                                    | rds:param:listAll                    | -            |
| POST /v3/{project_id}/configurations                                                                                                                                   | rds:param:createTemplate             | -            |
| PUT /v3/{project_id}/configurations/{config_id}                                                                                                                        | rds:param:updateTemplate             | -            |
| POST /v3/{project_id}/configurations/{config_id}/copy                                                                                                                  | rds:param:copy                       | -            |
| GET /v3/{project_id}/instances/{instance_id}/configuration-histories?offset={offset}&limit={limit}&start_time={start_time}&end_time={end_time}&param_name={param_name} | rds:param:listInstanceParamHistories | -            |
| GET /v3/{project_id}/instances/{instance_id}/configurations                                                                                                            | rds:instance:getParameter            | -            |
| GET /v3/{project_id}/configurations/{config_id}                                                                                                                        | rds:param:get                        | -            |
| DELETE /v3/{project_id}/configurations/{config_id}                                                                                                                     | rds:param:get                        | -            |

| API                                                                                                                 | Action                              | Dependencies |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------|--------------|
| POST /v3/{project_id}/instances/{instance_id}/extensions                                                            | rds:database:update                 | -            |
| GET /v3/{project_id}/instances/{instance_id}/extensions?database_name={database_name}&offset={offset}&limit={limit} | rds:database:list                   | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/extensions                                                          | rds:database:drop                   | -            |
| PUT /v3/{project_id}/instances/{instance_id}/parameter/{name}                                                       | rds:instance:updateParameter        | -            |
| GET /v3/{project_id}/instances/{instance_id}/parameter/{name}                                                       | rds:instance:getParameter           | -            |
| PUT /v3/{project_id}/instances/recycle-policy                                                                       | rds:instance:setRecycleBin          | -            |
| GET /v3/{project_id}/instances/recycle-policy                                                                       | rds:instance:listAll                | -            |
| GET /v3/{project_id}/recycle-instances?offset={offset}&limit={limit}                                                | rds:instance:listAll                | -            |
| POST /v3/{project_id}/instances/{instance_id}/tags/action                                                           | rds:instance:createTag              | -            |
| POST /v3/{project_id}/instances/{instance_id}/tags/action                                                           | rds:instance:deleteTag              | -            |
| GET /v3/{project_id}/tags                                                                                           | rds:tag:list                        | -            |
| GET /v3/{project_id}/quotas                                                                                         | rds:instance:listQuotas             | -            |
| GET /v3/{project_id}/jobs?id={id}                                                                                   | rds:task:listAll                    | -            |
| GET /v3/{project_id}/instances/{instance_id}/tasklist/detail?start_time={start_time}&end_time={end_time}            | rds:task:listAll                    | -            |
| PUT /v3/{project_id}/instances/{instance_id}/tde                                                                    | rds:instance:tde                    | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/delete-disaster-recovery                                            | rds:instance:deleteDisasterRecovery | -            |
| GET /v3/{project_id}/instances/{instance_id}/replay-delay/show                                                      | rds:instance:showReplayDelayStatus  | -            |
| PUT /v3/{project_id}/instances/{instance_id}/log-replay/update                                                      | rds:instance:switchLogReplay        | -            |

| API                                                                                                    | Action                               | Dependencies |
|--------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| GET /v3/{project_id}/instances/{instance_id}/recovery-time                                             | rds:instance:queryRecoveryTimeWindow | -            |
| PUT /v3/{project_id}/instances/{instance_id}/binlog/clear-policy                                       | rds:binlog:setPolicy                 | -            |
| GET /v3/{project_id}/instances/{instance_id}/binlog/clear-policy                                       | rds:binlog:get                       | -            |
| GET /v3/{project_id}/instances/diagnosis                                                               | rds:instance:listAll                 | -            |
| GET /v3/{project_id}/instances/diagnosis/info                                                          | rds:instance:listAll                 | -            |
| POST /v3/{project_id}/instances/{instance_id}/sql-limit                                                | rds:instance:update                  | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/sql-limit                                              | rds:instance:update                  | -            |
| PUT /v3/{project_id}/instances/{instance_id}/sql-limit/update                                          | rds:instance:update                  | -            |
| GET /v3/{project_id}/instances/{instance_id}/sql-limit?db_name={db_name}&offset={offset}&limit={limit} | rds:instance:get                     | -            |
| PUT /v3/{project_id}/instances/{instance_id}/sql-limit/switch                                          | rds:instance:update                  | -            |
| PUT /v3/{project_id}/instances/{instance_id}/unlock-node-readonly-status                               | rds:instance:update                  | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for RDS.

**Table 3-96** Resource types supported by RDS

| Resource Type | URN                                              |
|---------------|--------------------------------------------------|
| instance      | rds:<region>:<account-id>:instance:<instance-id> |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **rds:**) apply only to operations of the RDS service. For details, see [Table 4](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [condition operators](#).

The following table lists the condition keys that you can define in identity policies for RDS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-97** Service-specific condition keys supported by RDS

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                                                                |
|--------------------------------|---------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| rds:Encrypted                  | Boolean | Single-valued                 | Filters access permissions based on the tag key of whether to enable disk encryption transferred in the request parameter. |

| Service-specific Condition Key | Type    | Single-valued/Multivalued | Description                                                                                                                  |
|--------------------------------|---------|---------------------------|------------------------------------------------------------------------------------------------------------------------------|
| rds:BackupEnabled              | Boolean | Single-valued             | Filters access permissions based on the tag key of whether to enable the backup policy transferred in the request parameter. |

### 3.6.2 GaussDB

IAM provides system-defined policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.

- If this column includes a resource type, you must specify the URN in the Resource element of your policy statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by GaussDB, see [Resources](#).

- **Condition Key** contains keys that you can specify in the Condition element of a policy statement for GaussDB. If this column is empty (-), the action does not support any condition keys.

For details about the condition keys defined by GaussDB, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for identity policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for GaussDB.

**Table 3-98** Actions supported by GaussDB

| Action                      | Description                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias                 |
|-----------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------|
| gaussdb:backup:createBackup | Grants permission to create a manual backup for a DB instance. | write        | instance                    | -             | gaussdb:backup:create |
| gaussdb:backup:deleteBackup | Grants permission to delete a backup.                          | write        | instance                    | -             | gaussdb:backup:delete |
| gaussdb:backup:listAll      | Grants permission to query backups.                            | list         | instance                    | -             | gaussdb:backup:list   |

| Action                              | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                    | Alias                                                                                                                                                          |
|-------------------------------------|---------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gaussdb:instance:updateBackupPolicy | Grants permission to configure a backup policy.   | write        | instance                    | <b>gaussdb:BackupEnabled</b>                                                                                     | <ul style="list-style-type: none"> <li>gaussdb:backup:enable</li> <li>gaussdb:backup:switchTableBackup</li> <li>gaussdb:instance:modifyBackupPolicy</li> </ul> |
| gaussdb:param:applyParam            | Grants permission to apply a parameter template.  | write        | instance                    | -                                                                                                                | <ul style="list-style-type: none"> <li>gaussdb:param:apply</li> <li>gaussdb:param:modify</li> <li>gaussdb:instance:modifyParameter</li> </ul>                  |
| gaussdb:tag:create                  | Grants permission to add tags.                    | tagging      | instance                    | -                                                                                                                | gaussdb:instance:dealTag                                                                                                                                       |
| gaussdb:instance:bindEIP            | Grants permission to bind an EIP.                 | write        | instance                    | -                                                                                                                | <ul style="list-style-type: none"> <li>gaussdb:instance:bindPublicIp</li> <li>gaussdb:instance:modify</li> </ul>                                               |
| gaussdb:instance:check              | Grants permission to verify instance information. | read         | instance                    | -                                                                                                                | gaussdb:instance:list                                                                                                                                          |
| gaussdb:instance:createInstance     | Grants permission to create a DB instance.        | write        | instance                    | <ul style="list-style-type: none"> <li><b>gaussdb:BackupEnabled</b></li> <li><b>gaussdb:Encrypted</b></li> </ul> | rds:instance:create                                                                                                                                            |



| Action                                | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                |
|---------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------------------------|
| gaussdb:instance:createDatabase       | Grants permission to create a database.                                                         | write        | instance                    | -             | gaussdb:instance:modify                                                                              |
| gaussdb:instance:createDatabaseSchema | Grants permission to create a database schema.                                                  | write        | instance                    | -             | gaussdb:instance:modify                                                                              |
| gaussdb:instance:createDatabaseUser   | Grants permission to create a database account.                                                 | write        | instance                    | -             | gaussdb:instance:modify                                                                              |
| gaussdb:instance:deleteInstance       | Grants permission to delete a DB instance.                                                      | write        | instance                    | -             | gaussdb:instance:delete                                                                              |
| gaussdb:instance:get                  | Grants permission to query instance information.                                                | read         | instance                    | -             | gaussdb:instance:list                                                                                |
| gaussdb:instance:getBackupPolicy      | Grants permission to query an automated backup policy.                                          | read         | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> <li>gaussdb:backup:list</li> </ul> |
| gaussdb:instance:getBalanceStatus     | Grants permission to check whether host load is unbalanced due to a primary/standby switchover. | read         | instance                    | -             | gaussdb:instance:list                                                                                |

| Action                                  | Description                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias                   |
|-----------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------|
| gaussdb:instance:getDiskUsage           | Grants permission to query disk usage.                              | read         | instance                    | -             | gaussdb:instance:list   |
| gaussdb:instance:getRecyclePolicy       | Grants permission to query the recycling policy.                    | read         | instance                    | -             | gaussdb:instance:list   |
| gaussdb:instance:downloadSslCert        | Grants permission to download the SSL certificate of a DB instance. | read         | instance                    | -             | gaussdb:instance:list   |
| gaussdb:instance:grantDatabasePrivilege | Grants permission to authorize a database account.                  | write        | instance                    | -             | gaussdb:instance:modify |
| gaussdb:instance:listAll                | Grants permission to query DB instances.                            | list         | instance                    | -             | gaussdb:instance:list   |
| gaussdb:instance:listPublicips          | Grants permission to query EIPs bound to a DB instance.             | list         | instance                    | -             | gaussdb:instance:list   |
| gaussdb:instance:listComponents         | Grants permission to query instance components.                     | list         | instance                    | -             | gaussdb:instance:list   |
| gaussdb:instance:listDatabases          | Grants permission to query databases.                               | list         | instance                    | -             | gaussdb:instance:list   |

| Action                                | Description                                            | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                                                                           |
|---------------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gaussdb:instance:listDatabaseUsers    | Grants permission to query database users.             | list         | instance                    | -             | gaussdb:instance:list                                                                                                                                           |
| gaussdb:tag:listAll                   | Grants permission to query resource tags.              | list         | instance                    | -             | gaussdb:instance:list                                                                                                                                           |
| gaussdb:quota:listAll                 | Grants permission to query quotas.                     | list         | instance                    | -             | gaussdb:instance:list                                                                                                                                           |
| gaussdb:instance:listRecoverableTimes | Grants permission to query the restoration time range. | list         | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> <li>gaussdb:backup:list</li> </ul>                                                            |
| gaussdb:instance:listSchemas          | Grants permission to query database schemas.           | list         | instance                    | -             | gaussdb:instance:list                                                                                                                                           |
| gaussdb:instance:renameInstance       | Grants permission to change a DB instance name.        | write        | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> <li>gaussdb:instance:rename</li> </ul>                                                      |
| gaussdb:instance:resetPassword        | Grants permission to reset a database password.        | write        | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> <li>gaussdb:instance:modifyPasswd</li> <li>gaussdb:instance:modifyDatabasePasswd</li> </ul> |

| Action                            | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                                                                 |
|-----------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| gaussdb:instance:resizeFlavor     | Grants permission to change vCPUs and memory of a DB instance.             | write        | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> <li>gaussdb:instance:modifySpec</li> </ul>                                        |
| gaussdb:instance:restartInstance  | Grants permission to reboot a DB instance.                                 | write        | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> <li>gaussdb:instance:restart</li> </ul>                                           |
| gaussdb:instance:setRecyclePolicy | Grants permission to modify the recycling policy.                          | write        | instance                    | -             | gaussdb:instance:modifyBackupPolicy                                                                                                                   |
| gaussdb:instance:switchShard      | Grants permission to switch roles of the primary and standby DN in shards. | write        | instance                    | -             | gaussdb:instance:modify                                                                                                                               |
| gaussdb:instance:extend           | Grants permission to perform scale-out operations.                         | write        | instance                    | -             | gaussdb:instance:modifySpec                                                                                                                           |
| gaussdb:parameter:update          | Grants permission to modify a parameter template.                          | write        | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:parameter:modify</li> <li>gaussdb:instance:modify</li> <li>gaussdb:instance:modifyParameter</li> </ul> |

| Action                    | Description                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                |
|---------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------------------------|
| gaussdb:param:check       | Grants permission to check a parameter template.               | read         | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:param:list</li> <li>gaussdb:instance:list</li> </ul>  |
| gaussdb:param:copy        | Grants permission to replicate a parameter template.           | write        | instance                    | -             | gaussdb:param:create                                                                                 |
| gaussdb:param:createParam | Grants permission to create a parameter template.              | write        | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:param:create</li> <li>gaussdb:param:modify</li> </ul> |
| gaussdb:param:deleteParam | Grants permission to delete a parameter template.              | write        | instance                    | -             | gaussdb:param:delete                                                                                 |
| gaussdb:param:get         | Grants permission to query details about a parameter template. | read         | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:param:list</li> <li>gaussdb:instance:list</li> </ul>  |
| gaussdb:param:compare     | Grants permission to compare two parameter templates.          | read         | instance                    | -             | gaussdb:param:list                                                                                   |
| gaussdb:param:listAll     | Grants permission to query parameter templates.                | list         | instance                    | -             | <ul style="list-style-type: none"> <li>gaussdb:param:list</li> <li>gaussdb:instance:list</li> </ul>  |

| Action               | Description                                      | Access Level | Resource Type (*: required) | Condition Key | Alias                 |
|----------------------|--------------------------------------------------|--------------|-----------------------------|---------------|-----------------------|
| gaussdb:param:reset  | Grants permission to reset a parameter template. | write        | instance                    | -             | gaussdb:param:modify  |
| gaussdb:quota:update | Grants permission to modify quotas.              | write        | instance                    | -             | gaussdb:quota:modify  |
| gaussdb:task:listAll | Grants permission to query tasks.                | list         | instance                    | -             | gaussdb:instance:list |
| gaussdb:task:delete  | Grants permission to delete a task record.       | write        | instance                    | -             | gaussdb:instance:list |
| gaussdb:task:get     | Grants permission to query task details.         | read         | instance                    | -             | gaussdb:instance:list |

Each API of GaussDB usually supports one or more actions. The following table lists the supported actions and dependencies.

**Table 3-99** Instance management

| Permission             | API                                             | Action                          | Dependencies |
|------------------------|-------------------------------------------------|---------------------------------|--------------|
| Creating a DB instance | POST /v3/{project_id}/instances                 | gaussdb:instance:createInstance | -            |
| Deleting a DB instance | DELETE /v3/{project_id}/instances/{instance_id} | gaussdb:instance:delete         | -            |
| Querying DB instances  | GET /v3/{project_id}/instances                  | gaussdb:instance:listAll        | -            |

| Permission                                                                   | API                                                                                   | Action                            | Dependencies |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------|--------------|
| Resetting a database password                                                | POST /v3/{project_id}/instances/{instance_id}/password                                | gaussdb:instance:resetPassword    | -            |
| Changing a DB instance name                                                  | PUT /v3/{project_id}/instances/{instance_id}/name                                     | gaussdb:instance:rename           | -            |
| Rebooting a DB instance                                                      | POST /v3/{project_id}/instances/{instance_id}/restart                                 | gaussdb:instance:restart          | -            |
| Switching roles of the primary and standby DN in shards                      | POST /v3/{project_id}/instances/{instance_id}/switch-shard                            | gaussdb:instance:switchShard      | -            |
| Querying the components of a DB instance                                     | GET /v3/{project_id}/instances/{instance_id}/components                               | gaussdb:instance:listComponents   | -            |
| Changing vCPUs and memory of a DB instance                                   | PUT /v3/{project_id}/instance/{instance_id}/flavor                                    | gaussdb:instance:resizeFlavor     | -            |
| Checking whether host load is unbalanced due to a primary/standby switchover | GET /v3/{project_id}/instances/{instance_id}/balance                                  | gaussdb:instance:getBalanceStatus | -            |
| Querying solution template settings                                          | GET /v3/{project_id}/deployment-form                                                  | gaussdb:instance:listAll          | -            |
| Querying EIPs bound to a DB instance                                         | GET /v3/{project_id}/instances/{instance_id}/public-ips?offset={offset}&limit={limit} | gaussdb:instance:listPublicIps    | -            |

| Permission                                                     | API                                                                     | Action                           | Dependencies |
|----------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------|--------------|
| Validating password strength                                   | POST /v3/{project_id}/weak-password-verification                        | gaussdb:instance:check           | -            |
| Binding or unbinding an EIP                                    | POST /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/public-ip | gaussdb:instance:bindPublicIp    | -            |
| Querying the SSL certificate download address of a DB instance | GET /v3/{project_id}/instances/{instance_id}/ssl-cert/download-link     | gaussdb:instance:downloadSslCert | -            |
| Querying the instance quotas of a tenant                       | GET /v3/{project_id}/project-quotas?type={type}                         | gaussdb:quota:listAll            | -            |

**Table 3-100** Parameter configuration

| Permission                                      | API                                                               | Action                    | Dependencies |
|-------------------------------------------------|-------------------------------------------------------------------|---------------------------|--------------|
| Obtaining parameter templates                   | GET /v3/{project_id}/configurations?offset={offset}&limit={limit} | gaussdb:param:listAll     | -            |
| Obtaining parameters of a specified DB instance | GET /v3/{project_id}/instances/{instance_id}/configurations       | gaussdb:instance:get      | -            |
| Modifying parameters of a specified DB instance | PUT /v3/{project_id}/instances/{instance_id}/configurations       | gaussdb:param:update      | -            |
| Creating a parameter template                   | POST /v3/{project_id}/configurations                              | gaussdb:param:createParam | -            |
| Deleting a parameter template                   | DELETE /v3/{project_id}/configurations/{config_id}                | gaussdb:param:delete      | -            |



| Permission                                                     | API                                                                  | Action                   | Dependencies |
|----------------------------------------------------------------|----------------------------------------------------------------------|--------------------------|--------------|
| Querying details about a parameter template                    | GET /v3/{project_id}/configurations/{config_id}                      | gaussdb:param:get        | -            |
| Replicating a parameter template                               | POST /v3/{project_id}/configurations/{config_id}/copy                | gaussdb:param:copy       | -            |
| Resetting a parameter template                                 | POST /v3/{project_id}/configurations/{config_id}/reset               | gaussdb:param:reset      | -            |
| Obtaining the differences of two parameter templates           | POST /v3/{project_id}/configurations/comparison                      | gaussdb:param:compare    | -            |
| Querying instances that a parameter template can be applied to | GET /v3/{project_id}/configurations/{config_id}/applicable-instances | gaussdb:instance:listAll | -            |
| Checking whether a parameter template name is unique           | GET /v3/{project_id}/configurations/name-validation?name={name}      | gaussdb:param:check      | -            |
| Applying a parameter template                                  | PUT /v3/{project_id}/configurations/{config_id}/apply                | gaussdb:param:apply      | -            |
| Querying application records of a parameter template           | GET /v3/{project_id}/configurations/{config_id}/applied-histories    | gaussdb:param:listAll    | -            |
| Querying the change history of a parameter template            | GET /v3/{project_id}/configurations/{config_id}/histories            | gaussdb:param:listAll    | -            |

**Table 3-101** Backup management

| Permission                                                                                           | API                                                                                                                                                                              | Action                                | Dependencies |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|--------------|
| Configuring an automated backup policy                                                               | PUT /v3/{project_id}/instances/{instance_id}/backups/policy                                                                                                                      | gaussdb:instance:updateBackupPolicy   | -            |
| Querying an automated backup policy                                                                  | GET /v3/{project_id}/instances/{instance_id}/backups/policy                                                                                                                      | gaussdb:instance:getBackupPolicy      | -            |
| Querying backups                                                                                     | GET /v3/{project_id}/backups?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin_time}&end_time={end_time} | gaussdb:backup:listAll                | -            |
| Creating a manual backup                                                                             | POST /v3/{project_id}/backups                                                                                                                                                    | gaussdb:backup:create                 | -            |
| Deleting a manual backup                                                                             | DELETE /v3/{project_id}/backups/{backup_id}                                                                                                                                      | gaussdb:backup:delete                 | -            |
| Querying the restoration time range                                                                  | GET /v3/{project_id}/instances/{instance_id}/restore-time?date={date}                                                                                                            | gaussdb:instance:listRecoverableTimes | -            |
| Restoring data to a new DB instance                                                                  | POST /v3/{project_id}/instances                                                                                                                                                  | gaussdb:instance:createInstance       | -            |
| Querying instances that can be used for backups and restorations                                     | GET /v3/{project_id}/restorable-instances                                                                                                                                        | gaussdb:instance:listAll              | -            |
| Querying the information of the original instance based on a specific point of time or a backup file | GET /v3/{project_id}/instance-snapshot?instance_id={instance_id}&backup_id={backup_id}&restore_time={restore_time}                                                               | gaussdb:instance:get                  | -            |

**Table 3-102** DB engine versions and specifications

| Permission                                                   | API                                                                                                                  | Action                       | Dependencies |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------|--------------|
| Querying DB engine versions                                  | GET /v3/{project_id}/datastore/versions                                                                              | gaussdb:instance:list<br>All | -            |
| Querying instance specifications                             | GET /v3/{project_id}/flavors?limit={limit}&offset={offset}&ha_mode={ha_mode}&version={version}&spec_code={spec_code} | gaussdb:instance:list<br>All | -            |
| Querying DB engines                                          | GET /v3/{project_id}/datastores                                                                                      | gaussdb:instance:list<br>All | -            |
| Querying specifications that a DB instance can be changed to | GET /v3/{project_id}/instances/{instance_id}/available-flavors                                                       | gaussdb:instance:list<br>All | -            |

**Table 3-103** Database and account management

| Permission                     | API                                                        | Action                                  | Dependencies |
|--------------------------------|------------------------------------------------------------|-----------------------------------------|--------------|
| Creating a database            | POST /v3/{project_id}/instances/{instance_id}/database     | gaussdb:instance:createDatabase         | -            |
| Creating a database account    | POST /v3/{project_id}/instances/{instance_id}/db-user      | gaussdb:instance:createDatabaseUser     | -            |
| Creating a database schema     | POST /v3/{project_id}/instances/{instance_id}/schema       | gaussdb:instance:createDatabaseSchema   | -            |
| Authorizing a database account | POST /v3/{project_id}/instances/{instance_id}/db-privilege | gaussdb:instance:grantDatabasePrivilege | -            |

| Permission                                  | API                                                           | Action                             | Dependencies |
|---------------------------------------------|---------------------------------------------------------------|------------------------------------|--------------|
| Resetting a password for a database account | PUT /v3/{project_id}/instances/{instance_id}/db-user/password | gaussdb:instance:resetPassword     | -            |
| Querying databases                          | GET /v3/{project_id}/instances/{instance_id}/databases        | gaussdb:instance:listDatabases     | -            |
| Querying database accounts                  | GET /v3/{project_id}/instances/{instance_id}/db-users         | gaussdb:instance:listDatabaseUsers | -            |
| Querying database schemas                   | GET /v3/{project_id}/instances/{instance_id}/schemas          | gaussdb:instance:listSchemas       | -            |

**Table 3-104** Tag management

| Permission                           | API                                                | Action              | Dependencies |
|--------------------------------------|----------------------------------------------------|---------------------|--------------|
| Querying tags of a specific instance | GET /v3/{project_id}/instances/{instance_id}/tags  | gaussdb:tag:listAll | -            |
| Querying tags of a project           | GET /v3/{project_id}/tags                          | gaussdb:tag:listAll | -            |
| Querying predefined tags             | GET /v3/{project_id}/predefined-tags               | gaussdb:tag:listAll | -            |
| Adding tags to a DB instance         | POST /v3/{project_id}/instances/{instance_id}/tags | gaussdb:tag:create  | -            |

**Table 3-105** Storage management

| Permission                                  | API                                                                   | Action                        | Dependencies |
|---------------------------------------------|-----------------------------------------------------------------------|-------------------------------|--------------|
| Querying the storage usage of a DB instance | GET /v3/{project_id}/instances/{instance_id}/volume-usage             | gaussdb:instance:getDiskUsage | -            |
| Querying the database disk type             | GET /v3/{project_id}/storage-type?version={version}&ha_mode={ha_mode} | gaussdb:instance:listAll      | -            |

**Table 3-106** Quota management

| Permission                          | API                                             | Action                | Dependencies |
|-------------------------------------|-------------------------------------------------|-----------------------|--------------|
| Modifying enterprise project quotas | PUT /v3/{project_id}/enterprise-projects/quotas | gaussdb:quota:update  | -            |
| Querying enterprise project quotas  | GET /v3/{project_id}/enterprise-projects/quotas | gaussdb:quota:listAll | -            |

**Table 3-107** Task management

| Permission                 | API                                   | Action               | Dependencies |
|----------------------------|---------------------------------------|----------------------|--------------|
| Obtaining task information | GET /v3/{project_id}/jobs?id={id}     | gaussdb:task:get     | -            |
| Querying tasks             | GET /v3/{project_id}/tasks            | gaussdb:task:listAll | -            |
| Deleting a task record     | DELETE /v3/{project_id}/jobs/{job_id} | gaussdb:task:delete  | -            |

**Table 3-108** Recycle bin

| Permission                                          | API                                    | Action                            | Dependencies |
|-----------------------------------------------------|----------------------------------------|-----------------------------------|--------------|
| Modifying the recycling policy                      | PUT /v3/{project_id}/recycle-policy    | gaussdb:instance:setRecyclePolicy | -            |
| Querying the recycling policy                       | GET /v3/{project_id}/recycle-policy    | gaussdb:instance:getRecyclePolicy | -            |
| Querying all DB engine instances in the recycle bin | GET /v3/{project_id}/recycle-instances | gaussdb:instance:listAll          | -            |

**Table 3-109** DR management

| Permission                                                 | Action                             | Authorization Scope                                                                     | API                                                                    |
|------------------------------------------------------------|------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Querying instances that can establish a DR relationship    | gaussdb:disasterRecovery:list      | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{project_id}/disaster/instances/candidates                       |
| Checking DR operations                                     | gaussdb:disasterRecovery:list      | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{project_id}/instances/{instance_id}/disaster/operation-precheck |
| Querying instance DR status                                | gaussdb:disasterRecovery:list      | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{project_id}/instances/{instance_id}/disaster/monitor            |
| Querying instances that have established a DR relationship | gaussdb:disasterRecovery:list      | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{project_id}/disaster/relations                                  |
| Establishing a DR relationship                             | gaussdb:disasterRecovery:construct | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{projectId}/instances/{instanceId}/disaster/construct            |

| Permission                                  | Action                              | Authorization Scope                                                                     | API                                                                                        |
|---------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Promoting the DR instance to primary        | gaussdb:disasterRecovery:failover   | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.2/{projectId}/instances/{instanceId}/failover                                          |
| Deleting a DR relationship                  | gaussdb:disasterRecovery:release    | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{projectId}/instances/{instanceId}/disaster/relations/{synchronizationId}/release    |
| Switching roles of primary and DR instances | gaussdb:disasterRecovery:switchover | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{projectId}/instances/{instanceId}/disaster/relations/{synchronizationId}/switchover |
| Re-establishing a DR relationship           | gaussdb:disasterRecovery:construct  | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{projectId}/instances/{instanceId}/disaster/relations/{synchronizationId}/restore    |
| Enabling DR drill                           | gaussdb:disasterRecovery:simulation | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{projectId}/instances/{instanceId}/disaster-simulation/start                         |
| Disabling DR drill                          | gaussdb:disasterRecovery:simulation | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.1/{projectId}/instances/{instanceId}/disaster-simulation/stop                          |
| Enabling log cache                          | gaussdb:disasterRecovery:keeplog    | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3/{projectId}/instances/{instanceId}/disaster-data-cache/start                           |
| Disabling log cache                         | gaussdb:disasterRecovery:keeplog    | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3/{projectId}/instances/{instanceId}/disaster-data-cache/stop                            |

| Permission                                                 | Action                              | Authorization Scope                                                                     | API                                                                     |
|------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Querying instances that have established a DR relationship | gaussdb:disasterRecovery:list       | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/disaster-recovery/relations                          |
| Querying instance DR status                                | gaussdb:disasterRecovery:list       | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/monitor    |
| Resetting DR configurations                                | gaussdb:disasterRecovery:construct  | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/instances/{instance_id}/reset-dr-config              |
| Establishing a DR relationship                             | gaussdb:disasterRecovery:construct  | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/construct  |
| Promoting the DR instance to primary                       | gaussdb:disasterRecovery:failover   | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/failover   |
| Deleting a DR relationship                                 | gaussdb:disasterRecovery:release    | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/release    |
| Switching roles of primary and DR instances                | gaussdb:disasterRecovery:switchover | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/switchover |
| Re-establishing a DR relationship                          | gaussdb:disasterRecovery:construct  | <ul style="list-style-type: none"> <li>Supported: VDC resource set (project)</li> </ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/restore    |



| Permission          | Action                              | Authorization Scope                                                                   | API                                                                           |
|---------------------|-------------------------------------|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Enabling DR drill   | gaussdb:disasterRecovery:simulation | <ul style="list-style-type: none"><li>Supported: VDC resource set (project)</li></ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/simulation-start |
| Disabling DR drill  | gaussdb:disasterRecovery:simulation | <ul style="list-style-type: none"><li>Supported: VDC resource set (project)</li></ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/simulation-stop  |
| Enabling log cache  | gaussdb:disasterRecovery:keeplog    | <ul style="list-style-type: none"><li>Supported: VDC resource set (project)</li></ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/keep-log-start   |
| Disabling log cache | gaussdb:disasterRecovery:keeplog    | <ul style="list-style-type: none"><li>Supported: VDC resource set (project)</li></ul> | /v3.5/{project_id}/instances/{instance_id}/disaster-recovery/keep-log-stop    |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-110](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for GaussDB.

**Table 3-110** Resource types supported by GaussDB

| Resource Type | URN                                                  |
|---------------|------------------------------------------------------|
| instance      | gaussdb:<region>:<account-id>:instance:<instance-id> |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global or service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **gaussdb:**) only apply to operations of the STS service. For details, see [Table 3-111](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

The following table lists the condition keys that you can define in identity policies for GaussDB. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-111** Service-specific condition keys supported by GaussDB

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                                                                                                              |
|--------------------------------|---------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gaussdb:Backup Enabled         | boolean | Single-valued                 | Filter access permissions based on the tag key of whether to enable the backup policy transferred in the request parameter. Select <b>Default</b> for <b>Qualifier</b> . |

| Service-specific Condition Key | Type    | Single-valued/Multivalued | Description                                                                                                                                                            |
|--------------------------------|---------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gaussdb:Encrypted              | boolean | Single-valued             | Filter access permissions based on the tag key of whether to enable disk encryption transferred in the request parameter. Select <b>Default</b> for <b>Qualifier</b> . |

### 3.6.3 Document Database Service (DDS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.

- If this column includes a resource type, you must specify the URN in the Resource element of your statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DDS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DDS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DDS.

**Table 3-112** Actions supported by DDS

| Action                 | Description                                               | Access Level          | Resource Type (*: required) | Condition Key | Aliases |
|------------------------|-----------------------------------------------------------|-----------------------|-----------------------------|---------------|---------|
| dds:instance:setSsl    | Grants permission to enable or disable SSL.               | permission_management | instance                    | -             | -       |
| dds:instance:unbindEIP | Grants permission to unbind an EIP from a DB instance.    | write                 | -                           | -             | -       |
| dds:instance:migrateAz | Grants permission to migrate a DB instance to another AZ. | write                 | -                           | -             | -       |

| Action                         | Description                                                          | Access Level          | Resource Type (*: required) | Condition Key | Aliases |
|--------------------------------|----------------------------------------------------------------------|-----------------------|-----------------------------|---------------|---------|
| dds:instance:listMigrateAZ     | Grants permission to query AZs to which an instance can be migrated. | list                  | -                           | -             | -       |
| dds:instance:updateIp          | Grants permission to change the private IP address of a DB instance. | write                 | instance                    | -             | -       |
| dds:instance:bindEIP           | Grants permission to bind an EIP to a DB instance.                   | write                 | -                           | -             | -       |
| dds:instance:resetPassword     | Grants permission to reset the password of a database user.          | write                 | instance                    | -             | -       |
| dds:instance:checkPassword     | Grants permission to check a database password.                      | read                  | instance                    | -             | -       |
| dds:instance:updatePort        | Grants permission to change a database port.                         | write                 | instance                    | -             | -       |
| dds:backup:download            | Grants permission to download backups.                               | read                  | instance                    | -             | -       |
| dds:instance:setAuditLogPolicy | Grants permission to configure an audit log policy.                  | permission_management | instance                    | -             | -       |

| Action                         | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Aliases |
|--------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------|
| dds:instance:getAuditLogPolicy | Grants permission to query the audit log policy.                | list         | instance                    | -                                     | -       |
| dds:instance:listAuditLog      | Grants permission to query audit logs.                          | list         | instance                    | -                                     | -       |
| dds:instance:listSlowLog       | Grants permission to query slow query logs.                     | list         | instance                    | -                                     | -       |
| dds:instance:downloadSlowLog   | Grants permission to download slow query logs.                  | read         | instance                    | -                                     | -       |
| dds:instance:listErrorLog      | Grants permission to query error logs.                          | list         | instance                    | -                                     | -       |
| dds:instance:downloadErrorLog  | Grants permission to download error logs.                       | read         | instance                    | -                                     | -       |
| dds:configuration:delete       | Grants permission to delete a parameter template.               | write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -       |
| dds:configuration:update       | Grants permission to modify parameters in a parameter template. | write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -       |
| dds:backup:listAll             | Grants permission to query backups.                             | list         | -                           | -                                     | -       |

| Action                           | Description                                                                                            | Access Level | Resource Type (*: required) | Condition Key         | Aliases |
|----------------------------------|--------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------|---------|
| dds:instance:updateConfiguration | Grants permission to modify the parameter template configuration of a DB instance or DB instance node. | write        | instance                    | -                     | -       |
| dds:instance:applyConfiguration  | Grants permission to apply a parameter template to a DB instance or DB instance node.                  | write        | -                           | -                     | -       |
| dds:instance:createIp            | Grants permission to create an IP address.                                                             | write        | -                           | -                     | -       |
| dds:backup:delete                | Grants permission to delete a backup.                                                                  | write        | -                           | -                     | -       |
| dds:instance:updateSecurityGroup | Grants permission to change the security group of a DB instance.                                       | write        | instance                    | -                     | -       |
| dds:configuration:listAll        | Grants permission to query parameter templates.                                                        | list         | -                           | g:EnterpriseProjectId | -       |

| Action                                      | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                | Aliases |
|---------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|------------------------------|---------|
| dds:instance:getConfiguration               | Grants permission to query parameters of a specified DB instance.      | read         | instance                    | -                            | -       |
| dds:configuration:get                       | Grants permission to query details about a parameter template.         | read         | -                           | <b>g:EnterpriseProjectId</b> | -       |
| dds:instance:updateSpec                     | Grants permission to change the instance class.                        | write        | instance                    | -                            | -       |
| dds:instance:getSecondLevelMonitoringConfig | Grants permission to query the configuration of Monitoring by Seconds. | read         | instance                    | -                            | -       |
| dds:instance:setSecondLevelMonitoringConfig | Grants permission to enable Monitoring by Seconds.                     | write        | instance                    | -                            | -       |
| dds:instance:switchover                     | Grants permission to perform a primary/secondary switchover.           | write        | instance                    | -                            | -       |
| dds:instance:extendVolume                   | Grants permission to scale up storage space of a DB instance.          | write        | instance                    | -                            | -       |



| Action                               | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key | Aliases |
|--------------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------|
| dds:instance:listAll                 | Grants permission to query DB instances.                                          | list         | -                           | -             | -       |
| dds:instance:setRecyclePolicy        | Grants permission to configure a recycling policy.                                | write        | -                           | -             | -       |
| dds:instance:getRecyclePolicy        | Grants permission to query the recycling policy.                                  | read         | -                           | -             | -       |
| dds:instance:listRecycleInstances    | Grants permission to query DB instances in the recycle bin.                       | list         | -                           | -             | -       |
| dds:instance:getUpgradeDuration      | Grants permission to query the estimated database minor version upgrade duration. | read         | instance                    | -             | -       |
| dds:instance:getDiskUsage            | Grants permission to query disk usage.                                            | read         | instance                    | -             | -       |
| dds:configuration:listAppliedHistory | Grants permission to query application records of a parameter template.           | list         | -                           | -             | -       |

| Action                                 | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key | Aliases |
|----------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------|
| dds:configuration:listUpdatedHistory   | Grants permission to query change history of a parameter template.           | list         | -                           | -             | -       |
| dds:configuration:compare              | Grants permission to compare two parameter templates.                        | read         | -                           | -             | -       |
| dds:configuration:copy                 | Grants permission to replicate a parameter template.                         | write        | -                           | -             | -       |
| dds:configuration:reset                | Grants permission to reset a parameter template.                             | write        | -                           | -             | -       |
| dds:instance:getSslCertDownloadAddress | Grants permission to obtain the address for downloading the SSL certificate. | read         | instance                    | -             | -       |
| dds:instance:addNode                   | Grants permission to add nodes for a DB instance.                            | write        | instance                    | -             | -       |
| dds:instance:deleteEnlargeFailedNode   | Grants permission to delete an instance node that fails to be added.         | write        | instance                    | -             | -       |

| Action                      | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key | Aliases |
|-----------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------|
| dds:task:listAll            | Grants permission to query tasks.                                              | list         | -                           | -             | -       |
| dds:task:getDetail          | Grants permission to query details about a task.                               | read         | -                           | -             | -       |
| dds:instance:restart        | Grants permission to restart a DB instance.                                    | write        | instance                    | -             | -       |
| dds:instance:deleteAuditLog | Grants permission to delete audit logs.                                        | write        | instance                    | -             | -       |
| dds:instance:delete         | Grants permission to delete a DB instance.                                     | write        | instance                    | -             | -       |
| dds:instance:updateName     | Grants permission to change a DB instance name.                                | write        | instance                    | -             | -       |
| dds:instance:updateRemark   | Grants permission to change a DB instance description.                         | write        | instance                    | -             | -       |
| dds:instance:setTag         | Grants permission to add or delete tags of a specified DB instance in batches. | tagging      | instance                    | -             | -       |

| Action                                 | Description                                                 | Access Level          | Resource Type (*: required) | Condition Key         | Aliases |
|----------------------------------------|-------------------------------------------------------------|-----------------------|-----------------------------|-----------------------|---------|
| dds:instance:listTags                  | Grants permission to query tags of a specified DB instance. | read                  | -                           | -                     | -       |
| dds:instance:setBackupPolicy           | Grants permission to configure an automated backup policy.  | write                 | -                           | dds:BackupEnabled     | -       |
| dds:instance:getBackupPolicy           | Grants permission to query an automated backup policy.      | read                  | -                           | -                     | -       |
| dds:configuration:create               | Grants permission to create a parameter template.           | write                 | -                           | g:EnterpriseProjectId | -       |
| dds:instance:setSlowLogPlainTextStatus | Grants permission to enable or disable Show Original Log.   | permission_management | instance                    | -                     | -       |
| dds:instance:getSlowLogPlainTextStatus | Grants permission to query the status of Show Original Log. | read                  | instance                    | -                     | -       |
| dds:instance:downloadAuditLog          | Grants permission to download audit logs.                   | read                  | instance                    | -                     | -       |

| Action                               | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                      | Aliases |
|--------------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------|---------|
| dds:instance:create                  | Grants permission to create a DB instance.                                        | write        | -                           | <a href="#">dds:Encrypted</a><br><a href="#">dds:BackupEnabled</a> | -       |
| dds:instance:restore                 | Grants permission to restore data to the original DB instance.                    | write        | -                           | -                                                                  | -       |
| dds:backup:getRestoreTimeList        | Grants permission to query restoration time ranges.                               | read         | -                           | -                                                                  | -       |
| dds:backup:getRestoreCollections     | Grant permission to obtain the list of database collections that can be restored. | list         | -                           | -                                                                  | -       |
| dds:backup:getRestoreDatabases       | Grant permission to obtain the list of databases that can be restored.            | list         | -                           | -                                                                  | -       |
| dds:instance:getConnectionStatistics | Grants permission to query the number of connections to an instance.              | read         | instance                    | -                                                                  | -       |
| dds:instance:getQuotas               | Grants permission to query quotas.                                                | read         | -                           | -                                                                  | -       |

| Action                              | Description                                                | Access Level | Resource Type (*: required) | Condition Key | Aliases |
|-------------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------|---------|
| dds:instance:createDatabaseUser     | Grants permission to create a database user.               | write        | instance                    | -             | -       |
| dds:instance:getDatabaseUser        | Grants permission to query database users.                 | read         | instance                    | -             | -       |
| dds:instance:deleteDatabaseUser     | Grants permission to delete a database user.               | write        | instance                    | -             | -       |
| dds:instance:createDatabaseRole     | Grants permission to create a database role.               | write        | instance                    | -             | -       |
| dds:instance:deleteDatabaseRole     | Grants permission to delete a database role.               | write        | instance                    | -             | -       |
| dds:instance:getDatabaseRole        | Grants permission to query database roles.                 | read         | instance                    | -             | -       |
| dds:instance:setSourceSubnet        | Grants permission to configure network segments.           | write        | instance                    | -             | -       |
| dds:instance:upgradeDatabaseVersion | Grants permission to upgrade the version of a DB instance. | write        | instance                    | -             | -       |

| Action                           | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key | Aliases |
|----------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------|
| dds:backup:create                | Grants permission to create a manual backup for a DB instance.               | write        | -                           | -             | -       |
| dds:instance:deleteSession       | Grants permission to kill sessions of an instance node.                      | write        | -                           | -             | -       |
| dds:instance:listSession         | Grants permission to query sessions of an instance node.                     | list         | -                           | -             | -       |
| dds:instance:getShardingBalancer | Grants permission to query the cluster balancer.                             | read         | instance                    | -             | -       |
| dds:instance:setShardingBalancer | Grants permission to set the cluster balancer.                               | write        | instance                    | -             | -       |
| dds:instance:setBalancerWindow   | Grants permission to set the activity time window for DDS cluster balancing. | write        | instance                    | -             | -       |
| dds:instance:updateOpsWindow     | Grants permission to set the maintenance window of a DB instance.            | write        | instance                    | -             | -       |

| Action                            | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key | Aliases |
|-----------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------|
| dds:instance:listFlavors          | Grants permission to query specifications.                                         | read         | -                           | -             | -       |
| dds:instance:listStorageType      | Grants permission to query storage types.                                          | read         | -                           | -             | -       |
| dds:instance:listDatabaseVersion  | Grants permission to query the database version information.                       | read         | -                           | -             | -       |
| dds:tag:listAll                   | Grants permission to query all tags in a project.                                  | list         | -                           | -             | -       |
| dds:instance:reduceNode           | Grants permission to delete nodes from a cluster DB instance.                      | write        | instance                    | -             | -       |
| dds:instance:createDomainName     | Grants permission to create DNS.                                                   | write        | -                           | -             | -       |
| dds:instance:updateDomainName     | Grants permission to change a DNS name.                                            | write        | -                           | -             | -       |
| dds:instance:updateReplicaSetName | Grants permission to change the name of the replica set in the connection address. | write        | instance                    | -             | -       |



| Action                         | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key | Aliases |
|--------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------|
| dds:instance:getDetail         | Grants permission to query details about a DB instance.                       | read         | instance                    | -             | -       |
| dds:instance:getNodeList       | Grants permission to query instance nodes.                                    | read         | instance                    | -             | -       |
| dds:instance:updateTag         | Grants permission to change a DB instance tag.                                | tagging      | instance                    | -             | -       |
| dds:instance:deleteTag         | Grants permission to delete a DB instance tag.                                | tagging      | instance                    | -             | -       |
| dds:backup:get                 | Grants permission to query information about a backup.                        | read         | -                           | -             | -       |
| dds:offsiteBackup:listRegion   | Grants permission to obtain the remote backup region of a specified instance. | read         | -                           | -             | -       |
| dds:offsiteBackup:listInstance | Grants permission to obtain the cross-region backup instance.                 | read         | -                           | -             | -       |

| Action                        | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                         | Aliases |
|-------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------|
| dds:offsiteBackup:listAll     | Grants permission to obtain cross-region backups.                       | read         | -                           | -                                     | -       |
| dds:instance:saveLogConfig    | Grants permission to enable log reporting for DB instances in batches.  | write        | -                           | -                                     | -       |
| dds:instance:deleteLogConfig  | Grants permission to disable log reporting for DB instances in batches. | write        | -                           | -                                     | -       |
| dds:backup:stop               | Grants permission to stop a backup.                                     | write        | -                           | -                                     | -       |
| dds:instance:createKillOpRule | Grants permission to create a SQL execution control rule.               | write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -       |
| dds:instance:deleteKillOpRule | Grants permission to delete a SQL execution control rule.               | write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -       |
| dds:instance:getKillOpRule    | Grants permission to query a SQL execution control rule.                | read         | instance                    | <a href="#">g:EnterpriseProjectId</a> | -       |

| Action                            | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Aliases |
|-----------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------|
| dds:instance:updateKillOpRule     | Grants permission to update a SQL execution control rule.                         | write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -       |
| dds:offsiteBackup:getBackupPolicy | Grants the permission to obtain the remote backup policy of a specified instance. | read         | instance                    | <a href="#">g:EnterpriseProjectId</a> | -       |
| dds:offsiteBackup:setBackupPolicy | Grants permission to configure a remote backup policy.                            | write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -       |

Each API of DDS usually supports one or more actions. [Table 3-113](#) lists the supported actions and dependencies.

**Table 3-113** Actions and dependencies supported by DDS APIs

| API                                                   | Action                                                                                                             | Dependencies |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------|
| POST /v3/{project_id}/instances                       | dds:instance:create<br>vpc:vpcs:list<br>vpc:vpcs:get<br>vpc:subnets:get<br>vpc:securityGroups:get<br>vpc:ports:get | -            |
| GET /v3/{project_id}/instances                        | dds:instance:listAll                                                                                               | -            |
| DELETE /v3/{project_id}/instances/{instance_id}       | dds:instance:delete                                                                                                | -            |
| POST /v3/{project_id}/instances/{instance_id}/restart | dds:instance:restart                                                                                               | -            |

| API                                                                 | Action                                                                                                              | Dependencies |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------|
| POST /v3/{project_id}/instances/{instance_id}/enlarge-volume        | dds:instance:extendVolume                                                                                           | -            |
| POST /v3/{project_id}/instances/{instance_id}/enlarge               | dds:instance:addNode<br>vpc:vpcs:list<br>vpc:vpcs:get<br>vpc:subnets:get<br>vpc:securityGroups:get<br>vpc:ports:get | -            |
| POST /v3/{project_id}/instances/{instance_id}/resize                | dds:instance:updateSpec                                                                                             | -            |
| POST /v3/{project_id}/instances/{instance_id}/switchover            | dds:instance:switchover                                                                                             | -            |
| POST /v3/{project_id}/instances/{instance_id}/switch-ssl            | dds:instance:setSSL                                                                                                 | -            |
| PUT /v3/{project_id}/instances/{instance_id}/modify-name            | dds:instance:updateName                                                                                             | -            |
| POST /v3/{project_id}/instances/{instance_id}/modify-port           | dds:instance:updatePort                                                                                             | -            |
| POST /v3/{project_id}/instances/{instance_id}/modify-security-group | dds:instance:updateSecurityGroup                                                                                    | -            |
| POST /v3/{project_id}/nodes/{node_id}/bind-eip                      | dds:instance:bindEIP                                                                                                | -            |
| POST /v3/{project_id}/nodes/{node_id}/unbind-eip                    | dds:instance:unbindEIP                                                                                              | -            |
| POST /v3/{project_id}/instances/{instance_id}/modify-internal-ip    | dds:instance:updateInternalIP                                                                                       | -            |
| POST /v3/{project_id}/instances/{instance_id}/create-ip             | dds:instance:createInternalIP                                                                                       | -            |
| GET /v3/{project_id}/instances/{instance_id}/migrate/az             | dds:instance:listMigrateAZ                                                                                          | -            |
| POST /v3/{project_id}/instances/{instance_id}/migrate               | dds:instance:migrateAZ                                                                                              | -            |
| GET /v3/{project_id}/nodes/{node_id}/sessions                       | dds:instance:listSessions                                                                                           | -            |
| POST /v3/{project_id}/nodes/{node_id}/session                       | dds:instance:deleteSession                                                                                          | -            |

| API                                                               | Action                                                                                                             | Dependencies |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------|
| GET /v3/{projectId}/instances/{instance_id}/conn-statistics       | dds:instance:getConnectionStatistics                                                                               | -            |
| POST /v3/{project_id}/backups                                     | dds:backup:create                                                                                                  | -            |
| DELETE /v3/{project_id}/backups/{backups_id}                      | dds:backup:delete                                                                                                  | -            |
| GET /v3/{project_id}/backups                                      | dds:backup:listAll                                                                                                 | -            |
| GET /v3/{project_id}/instances/{instance_id}/backups/policy       | dds:instance:getBackupPolicy                                                                                       | -            |
| PUT /v3/{project_id}/instances/{instance_id}/backups/policy       | dds:instance:setBackupPolicy                                                                                       | -            |
| POST /v3/{project_id}/instances                                   | dds:instance:create<br>vpc:vpcs:list<br>vpc:vpcs:get<br>vpc:subnets:get<br>vpc:securityGroups:get<br>vpc:ports:get | -            |
| GET /v3/{projectId}/backups/download-file                         | dds:backup:download                                                                                                | -            |
| GET /v3/{project_id}/instances/{instance_id}/restore-time         | dds:backup:getRestoreTimeList                                                                                      | -            |
| GET /v3/{project_id}/instances/{instance_id}/restore-database     | dds:backup:getRestoreDatabases                                                                                     | -            |
| GET /v3/{project_id}/instances/{instance_id}/restore-collection   | dds:backup:getRestoreCollections                                                                                   | -            |
| POST /v3/{project_id}/instances/recovery                          | dds:backup:restore                                                                                                 | -            |
| POST /v3/{project_id}/instances/{instance_id}/restore/collections | dds:backup:restore                                                                                                 | -            |
| GET /v3/{project_id}/configurations                               | dds:configuration:listAll                                                                                          | -            |
| POST /v3/{project_id}/configurations                              | dds:configuration:create                                                                                           | -            |
| DELETE /v3/{project_id}/configurations/{config_id}                | dds:configuration:delete                                                                                           | -            |
| GET /v3/{projectId}/configurations/{configId}                     | dds:configuration:get                                                                                              | -            |

| API                                                             | Action                           | Dependencies |
|-----------------------------------------------------------------|----------------------------------|--------------|
| PUT /v3/{project_id}/configurations/{config_id}                 | dds:configuration:update         | -            |
| PUT /v3/{project_id}/configurations/{config_id}/apply           | dds:instance:applyConfiguration  | -            |
| GET /v3/{project_id}/instances/{instance_id}/configurations     | dds:instance:getConfiguration    | -            |
| PUT /v3/{project_id}/instances/{instance_id}/configurations     | dds:instance:updateConfiguration | -            |
| GET /v3/{project_id}/instances/{instance_id}/slowlog            | dds:instance:listSlowLog         | -            |
| POST /v3/{project_id}/instances/{instance_id}/slowlog-download  | dds:instance:downloadSlowLog     | -            |
| GET /v3/{project_id}/instances/{instance_id}/errorlog           | dds:instance:listErrorLog        | -            |
| POST /v3/{project_id}/instances/{instance_id}/errorlog-download | dds:instance:downloadErrorLog    | -            |
| POST /v3/{project_id}/instances/{instance_id}/auditlog-policy   | dds:instance:setAuditLogPolicy   | -            |
| GET /v3/{project_id}/instances/{instance_id}/auditlog-policy    | dds:instance:getAuditLogPolicy   | -            |
| GET /v3/{project_id}/instances/{instance_id}/auditlog           | dds:instance:listAuditLog        | -            |
| POST /v3/{project_id}/instances/{instance_id}/auditlog-links    | dds:instance:downloadAuditLog    | -            |
| POST /v3/{project_id}/instances/{instance_id}/tags/action       | dds:instance:setTag              | -            |
| GET /v3/{project_id}/instances/{instance_id}/tags               | dds:instance:listTags            | -            |
| POST /v3/{project_id}/instances/{instance_id}/db-user           | dds:instance:createDatabaseUser  | -            |
| POST /v3/{project_id}/instances/{instance_id}/db-role           | dds:instance:createDatabaseRole  | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db-user         | dds:instance:deleteDatabaseUser  | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db-role         | dds:instance:deleteDatabaseRole  | -            |

| API                                                                 | Action                           | Dependencies |
|---------------------------------------------------------------------|----------------------------------|--------------|
| PUT /v3/{project_id}/instances/{instance_id}/reset-password         | dds:instance:resetPassword       | -            |
| GET /v3/{project_id}/instances/{instance_id}/db-user/detail         | dds:instance:getDatabaseUser     | -            |
| GET /v3/{project_id}/instances/{instance_id}/db-roles               | dds:instance:getDatabaseRole     | -            |
| GET /v3/{project_id}/instances/{instance_id}/balancer               | dds:instance:getShardingBalancer | -            |
| PUT /v3/{project_id}/instances/{instance_id}/balancer/{action}      | dds:instance:setShardingBalancer | -            |
| PUT /v3/{project_id}/instances/{instance_id}/balancer/active-window | dds:instance:setBalancerWindow   | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DDS.

**Table 3-114** Resource types supported by DDS

| Resource Type | URN                                                    |
|---------------|--------------------------------------------------------|
| instanceName  | dds:<region>:<account-id>:instanceName:<instance-name> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the

system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).

- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **dds:**) only apply to operations of the DDS service. For details, see [Table 4](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

#### Service-specific condition keys supported by DDS

The following table lists the condition keys that you can define in identity policies for DDS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-115** Service-specific condition keys supported by DDS

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                                      |
|--------------------------------|---------|-------------------------------|--------------------------------------------------------------------------------------------------|
| <b>dds:Encrypted</b>           | boolean | Single-valued                 | Filters access by the tag key that specifies whether to enable disk encryption in the request.   |
| <b>dds:BackupEnabled</b>       | boolean | Single-valued                 | Filters access by the tag key that specifies whether to enable the backup policy in the request. |

#### Examples of Condition Keys

- **dds:Encrypted**

For example, it indicates that disk encryption is required.

```
{ "Version": "5.0", "Statement": [ { "Effect": "Allow", "Action":
[ "dds:instance:create" ], "Condition": { "Bool": { "dds:Encrypted":
[ "true" ] } } } ] }
```

- **dds:BackupEnabled**

For example, it indicates that backup is required.



```
{ "Version": "5.0", "Statement": [ { "Effect": "Allow", "Action":
[ "dds:instance:create" ], "Condition": { "Bool": { "dds:BackupEnabled":
[ "true" ] } } } ] }
```

- `g:EnterpriseProjectId`

For example, it indicates that the enterprise project IDs must be the same.

```
{ "Version": "5.0", "Statement": [ { "Effect": "Allow", "Action":
[ "dds:instance:restart" ], "Condition": { "StringEquals":
{ "g:EnterpriseProjectId":
[ "d1a6b48538e74473af064856a0e03515" ] } } } ] }
```

### 3.6.4 Data Replication Service (DRS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DRS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DRS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for identity policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DRS.

**Table 3-116** Actions supported by DRS

| Action                           | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                           | Alias                         |
|----------------------------------|------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| drs:backupMigrationJob:createJob | Grants permission to create a backup migration task. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:backupMigrationJob:create |
| drs:backupMigrationJob:deleteJob | Grants permission to delete a backup migration task. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                      | drs:backupMigrationJob:delete |

| Action                                       | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                         |
|----------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| drs:backupMigrationJob:getJobDetail          | Grants permission to query details about a backup migration task.      | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:backupMigrationJob:get    |
| drs:backupMigrationJob:modifyOfflineTaskInfo | Grants permission to modify information about a backup migration task. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:backupMigrationJob:modify |
| drs:cloudDataGuardJob:getChartMonitor        | Grants permission to query report charts.                              | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:disasterRecoveryJob:get   |
| drs:cloudDataGuardJob:getDataGuardMonitor    | Grants permission to query DR monitoring data.                         | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:disasterRecoveryJob:get   |
| drs:cloudDataGuardJob:getLastDataDisplay     | Grants permission to query the last DR data.                           | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:dataGuardJob:list         |

| Action                                | Description                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                          |
|---------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| drs:cloudDataGuardJob:getRpoAndRto    | Grants permission to query the RPO and RTO of a specified task.    | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:dataGuardJob:list          |
| drs:compareJob:createDataCompareJob   | Grants permission to create a data-level table comparison task.    | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationCompareJob:create |
| drs:compareJob:createObjectCompareJob | Grants permission to create an object-level table comparison task. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationCompareJob:create |
| drs:compareJob:deleteDataCompareJob   | Grants permission to cancel a data-level table comparison task.    | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationCompareJob:delete |
| drs:migrationJob:getTopicInfo         | Grants permission to query information about all created topics.   | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get           |
| drs:migrationJob:listAllSmnInfo       | Grants permission to query all delivered information.              | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get           |

| Action                                    | Description                                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                    |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------|
| drs:configuration:getPublicIp             | Grants permission to query EIPs or EIP information.                                                 | list         | -                           | -                                                                                                              | drs:migrationJob:get     |
| drs:configuration:getVpcs                 | Grants permission to query VPCs.                                                                    | list         | -                           | -                                                                                                              | drs:migrationJob:get     |
| drs:configuration:listSubnets             | Grants permission to query subnets.                                                                 | list         | -                           | -                                                                                                              | drs:migrationJob:get     |
| drs:configuration:getFeatures             | Grants permission to query the feature whitelist.                                                   | list         | -                           | -                                                                                                              | drs:featureWhiteJob:list |
| drs:configuration:addTag                  | Grants permission to add tags.                                                                      | tagging      | -                           | -                                                                                                              | drs:tag:add              |
| drs:compareJob:exportAccountCompareResult | Grants permission to export and download the comparison result of an account-level comparison task. | list         | job                         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | drs:compareJob:list      |
| drs:compareJob:exportCompareReport        | Grants permission to download the comparison result.                                                | list         | job                         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | drs:compareJob:list      |

| Action                                     | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                      |
|--------------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| drs:configuration:getInstancesTag          | Grants permission to batch query tags.                                                | list         | -                           | -                                                                                                                                                  | drs:tag:get                |
| drs:compareJob:exportContentsCompareResult | Grants permission to export the comparison result of a value comparison task.         | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:compareJob:list        |
| drs:configuration:getProjectTags           | Grants permission to query project tags.                                              | list         | -                           | -                                                                                                                                                  | drs:tag:get                |
| drs:compareJob:exportLinesCompareResult    | Grants permission to export the comparison result of a row comparison task.           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:compareJob:list        |
| drs:compareJob:exportObjectsCompareResult  | Grants permission to export the comparison result of an object-level comparison task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:compareJob:list        |
| drs:compareJob:getAccountCompare           | Grants permission to query the overview of an account-level comparison task.          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:compareJob:getOverview |

| Action                                    | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                  |
|-------------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| drs:compareJob:getAccountCompareDetail    | Grants permission to query the details of an account-level comparison task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompareJob:getAccountDetails |
| drs:compareJob:getAccountCompareDetails   | Grants permission to query the details of an account-level comparison task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getAccountDetails       |
| drs:subscriptionJob:exportJobs            | Grants permission to export data subscription tasks.                        | list         | -                           | -                                                                                                                                                  | drs:subscriptionJob:get                |
| drs:compareJob:getAccountDetails          | Grants permission to query the overview of a row comparison task.           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompareJob:getAccountDetails |
| drs:compareJob:getCompareJobEstimatedTime | Grants permission to query the estimated time of a comparison task.         | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getEstimatedTime        |

| Action                                 | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                             |
|----------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| drs:compareJob:getComparePolicy        | Grants permission to query a comparison policy.                        | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthPolicyCompare:list      |
| drs:subscriptionJob:listJobs           | Grants permission to query data subscription tasks.                    | list         | -                           | -                                                                                                                                                  | drs:subscriptionJob:get           |
| drs:compareJob:getContentCompare       | Grants permission to query the overview of a value comparison task.    | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getContentOverview |
| drs:compareJob:getContentCompareDetail | Grants permission to query the details of a value comparison task.     | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getContentDetail   |
| drs:compareJob:getContentCompareDiff   | Grants permission to query the differences of a value comparison task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getContentDiff     |



| Action                                   | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|------------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:compareJob:getDataCompareDetail      | Grants permission to query the details of a row comparison task.                             | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompareJob:getLineDetail |
| drs:compareJob:getDataCompareResult      | Grants permission to query the comparison result of a data-level table comparison task.      | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getResult           |
| drs:compareJob:getFlowObjectsCompare     | Grants permission to query the overview of a dynamic object-level migration comparison task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:getCompareStruct  |
| drs:compareJob:getHealthCompareJobDetail | Grants permission to query details of a health comparison task.                              | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompareJob:list          |
| drs:compareJob:getLineCompare            | Grants permission to query the overview of a row comparison task.                            | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getLineOverview     |

| Action                                  | Description                                                                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:compareJob:getLineCompareDetail     | Grants permission to query the details of a row comparison task.                                                      | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getLineDetail       |
| drs:compareJob:getObjectCompare         | Grants permission to query the overview of an object-level migration comparison task based on the comparison task ID. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompareJob:getOverview   |
| drs:compareJob:getObjectsCompareDetail  | Grants permission to query the details of an object-level comparison task.                                            | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompareJob:getLineDetail |
| drs:compareJob:getObjectsMigrateCompare | Grants permission to query the overview of an object-level migration comparison task based on the task ID.            | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:list                |

| Action                                        | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                          |
|-----------------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| drs:compareJob:getObjectsMigrateCompareDetail | Grants permission to query the details of an object-level migration comparison task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getDetails      |
| drs:compareJob:getTableCompareDetail          | Grants permission to query the details of a data-level table comparison task.        | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:getContentsInfo |
| drs:compareJob:listDataCompare                | Grants permission to query data-level table comparison tasks.                        | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:CompareJob:list            |
| drs:compareJob:listHealthCompareJobs          | Grants permission to query the health comparison report list.                        | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompareJob:list      |
| drs:compareJob:modifyComparePolicy            | Grants permission to modify the comparison policy.                                   | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:healthCompare:modify       |

| Action                                      | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                         |
|---------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| drs:compareJob:startJob                     | Grants permission to immediately start a data-level table comparison task. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationCompareJob:start |
| drs:compareJob:stopJob                      | Grants permission to stop a comparison task.                               | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:healthCompare:stop        |
| drs:configuration:addDataTransformationInfo | Grants permission to add the data processing information.                  | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:dataTransformation:add    |
| drs:configuration:batchModifyTag            | Grants permission to batch add or modify tags.                             | tagging      | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:tags:delete               |

| Action                                         | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                         |
|------------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| drs:configuration:batchReplaceTags             | Grants permission to batch reset tags.                               | tagging      | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:tags:delete               |
| drs:configuration:checkDataTransformationInfo  | Grants permission to verify data processing information.             | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:dataTransformation:check  |
| drs:configuration:deleteDataTransformationInfo | Grants permission to delete data processing data.                    | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:dataTransformation:delete |
| drs:configuration:deleteSmnInfo                | Grants permission to delete a single piece of delivered information. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:action       |

| Action                                  | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                              |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:configuration:deleteSmnInfoForTopic | Grants permission to delete a single piece of delivered topic information.                            | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:action            |
| drs:configuration:deleteTag             | Grants permission to delete a tag.                                                                    | tagging      | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:tags:delete                    |
| drs:configuration:downloadTemplate      | Grants permission to download the Excel template before importing object information.                 | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:update            |
| drs:configuration:getAddColumns         | Grants permission to query data processing information (for many-to-one and column adding scenarios). | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationTransformationJob:get |

| Action                                      | Description                                                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:configuration:getAddColumnsFromDb       | Grants permission to query data processing information (for many-to-one and column adding scenarios) after the task is started. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationTransformationJob:get |
| drs:configuration:getFlavorInfo             | Grants permission to query the DB engine specifications.                                                                        | list         | -                           | -                                                                                                                                                  | drs:flavors:get                    |
| drs:backupMigrationJob:checkOfflineTaskName | Grants permission to verify the name of a backup migration task.                                                                | write        | -                           | -                                                                                                                                                  | drs:backupMigrationJob:check       |
| drs:configuration:getColumnInfo             | Grants permission to query the column information (column mapping and column filtering) of an object.                           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get               |

| Action                                      | Description                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|---------------------------------------------|-----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:configuration:getDatabaseName           | Grants permission to query the destination database name. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get               |
| drs:configuration:getDatabaseParams         | Grants permission to query database parameters.           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:databaseParameters:get         |
| drs:backupMigrationJob:exportJobList        | Grants permission to export backup migration tasks.       | list         | -                           | -                                                                                                                                                  | drs:backupMigrationJob:list        |
| drs:backupMigrationJob:getBackupFileDbList  | Grants permission to query databases in a backup file.    | list         | -                           | -                                                                                                                                                  | drs:backupMigrationJob:get         |
| drs:configuration:getDataTransformationData | Grants permission to query data processing data.          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationTransformationJob:get |
| drs:backupMigrationJob:getRedisInstList     | Grants permission to query Redis DB instances.            | list         | -                           | -                                                                                                                                                  | drs:backupMigrationJob:get         |



| Action                                      | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|---------------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:backupMigrationJob:listBuckets          | Grants permission to query buckets.                         | list         | -                           | -                                                                                                                                                  | drs:backupMigrationJob:get         |
| drs:backupMigrationJob:listJobs             | Grants permission to query backup migration tasks.          | list         | -                           | -                                                                                                                                                  | drs:backupMigrationJob:list        |
| drs:backupMigrationJob:listObsObject        | Grants permission to query objects in the current bucket.   | list         | -                           | -                                                                                                                                                  | drs:backupMigrationJob:get         |
| drs:configuration:getDataTransformationInfo | Grants permission to query data processing information.     | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationTransformationJob:get |
| drs:configuration:listFeature               | Grants permission to query supported features.              | list         | -                           | -                                                                                                                                                  | drs:supportFeature:get             |
| drs:configuration:listLinks                 | Grants permission to query available data flow information. | list         | -                           | -                                                                                                                                                  | drs:supportFeature:get             |

| Action                                             | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|----------------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:configuration:getEffectTime                    | Grants permission to query the database affected time of a specified task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:getEffectTime     |
| drs:configuration:getESConfig                      | Grants permission to query ElasticSearch configurations.                   | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get               |
| drs:configuration:getInstanceTag                   | Grants permission to query resource tags.                                  | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:tag:get                        |
| drs:configuration:getSupportDataTransformationType | Grants permission to query data processing data types.                     | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationTransformationJob:get |
| drs:configuration:getTableInfo                     | Grants permission to query the table structure and table data.             | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get               |

| Action                                 | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                     |
|----------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| drs:configuration:importSmnInfo        | Grants permission to enter the notification method and information.  | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:action   |
| drs:configuration:listTopics           | Grants permission to query Kafka topic information.                  | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:kafkaJob:get          |
| drs:configuration:modifyDatabaseParams | Grants permission to modify database parameters.                     | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:databaseParams:modify |
| drs:configuration:modifyESConfig       | Grants permission to modify ElasticSearch configurations.            | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get      |
| drs:configuration:modifySmnInfo        | Grants permission to modify the notification method and information. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:action   |

| Action                                   | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                                   |
|------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| drs:configuration:modifyTag              | Grants permission to modify resource tags.                     | tagging      | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:tag:modify                          |
| drs:configuration:modifyUserInfo         | Grants permission to update migration user information.        | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:modifyUserInfo         |
| drs:configuration:setMigrationTransSpeed | Grants permission to set the flow control of a migration task. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:setMigrationTransSpeed |
| drs:configuration:getInstanceNum         | Grants permission to query the number of tasks.                | list         | -                           | -                                                                                                                                                                                                                                               | drs:instances:list                      |
| drs:configuration:getInstanceQuotas      | Grants permission to query quotas.                             | list         | -                           | -                                                                                                                                                                                                                                               | drs:quota:get                           |

| Action                                         | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                         |
|------------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| drs:configuration:getQuota                     | Grants permission to query DRS quotas to a tenant.                     | list         | -                           | -                                                                                                                                                  | drs:quota:get                 |
| drs:migrationJob:batchDeleteJobs               | Grants permission to batch stop or delete tasks.                       | write        | -                           | -                                                                                                                                                  | drs:migrationJob:delete       |
| drs:configuration:updateDataTransformationInfo | Grants permission to update data processing information.               | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:dataTransformation:update |
| drs:migrationJob:addSubscribeJob               | Grants permission to create a yearly/monthly task.                     | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:action       |
| drs:migrationJob:associateSmnInfo              | Grants permission to associate the management-plane topic information. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:action       |
| drs:migrationJob:batchPauseJob                 | Grants permission to batch suspend tasks.                              | write        | -                           | -                                                                                                                                                  | drs:migrationJob:action       |

| Action                                       | Description                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias                    |
|----------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------|
| drs:migrationJob:batchPreCheckJob            | Grants permission to batch perform prechecks.                             | write        | -                           | -             | drs:migrationJob:action  |
| drs:migrationJob:batchRetryJob               | Grants permission to retry a task.                                        | write        | -                           | -             | drs:migrationJob:action  |
| drs:migrationJob:batchSetTransformation      | Grants permission to process synchronization objects.                     | write        | -                           | -             | drs:migrationJob:action  |
| drs:migrationJob:batchStartJob               | Grants permission to batch start tasks.                                   | write        | -                           | -             | drs:migrationJob:action  |
| drs:migrationJob:batchTestCluster-Connection | Grants permission to test connections in batches (cluster mode).          | write        | -                           | -             | drs:migrationJob:connect |
| drs:migrationJob:batchTestConnection         | Grants permission to test connections in batches.                         | write        | -                           | -             | drs:migrationJob:connect |
| drs:migrationJob:downloadBatchCreateTemplate | Grants permission to download the template for creating tasks in batches. | list         | -                           | -             | drs:migrationJob:get     |

| Action                                  | Description                                                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias                    |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------|
| drs:migrationJob:importBatchCreate-Jobs | Grants permission to import batch creation tasks.                                                         | write        | -                           | -             | drs:migrationJobs:create |
| drs:migrationJob:listAsyncJobDetail     | Grants permission to query details about the tasks created asynchronously in batches with a specified ID. | list         | -                           | -             | drs:migrationJob:get     |
| drs:migrationJob:listAsyncJobs          | Grants permission to query the list of tasks created asynchronously in batches.                           | list         | -                           | -             | drs:migrationJob:get     |
| drs:migrationJob:listJobInfo            | Grants permission to batch query task details by task ID.                                                 | list         | -                           | -             | drs:migrationJob:get     |
| drs:migrationJob:listJobStatus          | Grants permission to batch query task status by task ID.                                                  | list         | -                           | -             | drs:migrationJob:get     |

| Action                                        | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                 | Alias                   |
|-----------------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:asyncBatchCreateJobByAsyncId | Grants permission to asynchronously create tasks in batches.          | write        | job                         | <ul style="list-style-type: none"> <li>• drs:netType</li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:migrationJob:action |
| drs:migrationJob:getJobList                   | Grants permission to query tasks of a tenant.                         | list         | -                           | -                                                                                                                                                                                                             | drs:migrationJob:get    |
| drs:migrationJob:listPrecheckResult           | Grants permission to query the pre-check results of tasks in batches. | list         | -                           | -                                                                                                                                                                                                             | drs:migrationJob:get    |
| drs:migrationJob:selectDatabaseObject         | Grants permission to select the databases or tables to be migrated.   | write        | -                           | -                                                                                                                                                                                                             | drs:migrationJob:select |
| drs:configuration:listEPs                     | Grants permission to query enterprise projects.                       | list         | -                           | -                                                                                                                                                                                                             | drs:tag:get             |



| Action                                        | Description                                                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                          | Alias                    |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| drs:migrationJob:asyncBatchSaveJob            | Grants permission to submit the tasks created asynchronously in batches.                                   | write        | job                         | <ul style="list-style-type: none"> <li>• drs:netType</li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                          | drs:migrationJobs:create |
| drs:migrationJob:asyncBatchUpdateJobByAsyncId | Grants permission to update details about the tasks created asynchronously in batches with a specified ID. | write        | job                         | <ul style="list-style-type: none"> <li>• drs:netType</li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:migrationJob:action  |
| drs:migrationJob:batchCreateJob               | Grants permission to synchronously create tasks in batches.                                                | write        | job                         | <ul style="list-style-type: none"> <li>• drs:netType</li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                          | drs:migrationJobs:create |

| Action                              | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                          |
|-------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------------|
| drs:migrationJob:changeFlavor       | Grants permission to change specifications.                              | write        | job                         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | drs:migrationJob:action        |
| drs:migrationJob:getCesJobs         | Grants permission to query migration tasks.                              | list         | -                           | -                                                                                                              | drs:migrationJob:list          |
| drs:migrationJob:changeFlavorByNeed | Grants permission to change node specifications on the pay-per-use page. | write        | job                         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | drs:migrationJob:modify        |
| drs:compareJob:createJob            | Grants permission to create a comparison task.                           | write        | -                           | -                                                                                                              | drs:migrationCompareJob:create |
| drs:migrationJob:checkInheritJob    | Grants permission to determine whether a task can be inherited.          | write        | job                         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | drs:migrationJob:check         |
| drs:migrationJob:checkRestartPoint  | Grants permission to check resumable position.                           | write        | job                         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | drs:migrationJob:check         |

| Action                           | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                 | Alias                    |
|----------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| drs:migrationJob:checkTableExist | Grants permission to query whether the table structure and table data were found. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                            | drs:migrationJob:get     |
| drs:migrationJob:copyJobAction   | Grants permission to deliver a replication task.                                  | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                            | drs:migrationJob:check   |
| drs:migrationJob:createJob       | Grants permission to create an online migration task.                             | write        | job                         | <ul style="list-style-type: none"> <li>• drs:netType</li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:migrationJob:create  |
| drs:migrationJob:createJobs      | Grants permission to create a task.                                               | write        | job                         | <ul style="list-style-type: none"> <li>• drs:netType</li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:migrationJobs:create |

| Action                                         | Description                                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                      |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| drs:migrationJob:deleteColumnInfo              | Grants permission to delete the column information (column mapping and column filtering) of an object. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get       |
| drs:migrationJob:deleteJob                     | Grants permission to delete online migration task V1.                                                  | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:delete    |
| drs:migrationJob:downloadDbObjectTemplate      | Grants permission to download the object selection template.                                           | read         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update    |
| drs:migrationJob:endJob                        | Grants permission to stop an online migration task.                                                    | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:terminate |
| drs:migrationJob:exportAddedDeletedObjectsInfo | Grants permission to export added and deleted object information.                                      | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update    |

| Action                                 | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                    |
|----------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| drs:compareJob:getCompareResult        | Grants permission to query comparison results.                         | list         | -                           | -                                                                                                                                                  | drs:CompareJob:getResult |
| drs:migrationJob:exportErrorInfo       | Grants permission to export error information.                         | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update  |
| drs:migrationJob:exportObjectsSentInfo | Grants permission to export delivered object information.              | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update  |
| drs:migrationJob:getAccess             | Grants permission to query the allowed operations of a specified task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get     |
| drs:migrationJob:getAggregationTable   | Grants permission to query multi-table mapping in the memory.          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get     |

| Action                                       | Description                                                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|----------------------------------------------|------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:getCesJob                   | Grants permission to query migration task details.                                             | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |
| drs:migrationJob:getDbObjectCollectionStatus | Grants permission to obtain the result of submitting the query of database object information. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |
| drs:migrationJob:getDbObjects                | Grants permission to query database object information.                                        | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |
| drs:migrationJob:getDbObjectsCollectAsync    | Grants permission to submit the query of database object information.                          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |
| drs:migrationJob:getDbObjectTemplateProgress | Grants permission to query the progress of uploading the object import template.               | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update |

| Action                                          | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|-------------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:getDbObjectTemplateResult      | Grants permission to obtain the result of uploading the object import template. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update |
| drs:migrationJob:getFullJobDetails              | Grants permission to query details of a full synchronization task.              | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update |
| drs:migrationJob:getImportExcelProcess          | Grants permission to query the progress of parsing Excel files.                 | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update |
| drs:migrationJob:getIncrementalComponentDetails | Grants permission to query details about incremental components.                | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update |
| drs:migrationJob:getJob                         | Grants permission to query details about an online migration task.              | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |

| Action                                     | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                |
|--------------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| drs:migrationJob:getJobDetail              | Grants permission to query task details.                                                          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get                 |
| drs:migrationJob:getJobMeteringPrice       | Grants permission to query task price information.                                                | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:MigrationJob:getMeteringPrice    |
| drs:migrationJob:getObjectHasColumn        | Grants permission to query objects with column information (column mapping and column filtering). | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get                 |
| drs:migrationJob:getObjectsCompareOverview | Grants permission to query data-level streaming comparison.                                       | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:getStreamComparison |
| drs:migrationJob:getObjectSelectInfo       | Grants permission to query task object selection information.                                     | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get                 |



| Action                               | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                 |
|--------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| drs:migrationJob:getOperationInfo    | Grants permission to query the operation statistics of a specified task.           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get                  |
| drs:migrationJob:getProgress         | Grants permission to query the migration progress of a specified task.             | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:getSpecifiedProgress |
| drs:configuration:listDatabaseParams | Grants permission to query the parameters of the source and destination databases. | list         | -                           | -                                                                                                                                                  | drs:databaseParameters:get            |
| drs:migrationJob:getSmnInfo          | Grants permission to query a single piece of delivered information.                | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get                  |
| drs:migrationJob:getSmnInfoForTopic  | Grants permission to query a single piece of delivered topic information.          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get                  |

| Action                                      | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|---------------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:migrationJob:getSrcUsers                | Grants permission to query the migration users of the source database.                  | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:getSrcUsers       |
| drs:configuration:getOpenStreamResult       | Grants permission to query the result of enabling the stream mode.                      | list         | -                           | -                                                                                                                                                  | drs:migrationTransformationJob:get |
| drs:migrationJob:getSupportObject           | Grants permission to query whether a task supports object selection and column mapping. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get               |
| drs:migrationJob:getSupportSearchObjectType | Grants permission to query the object types that can be queried by a user.              | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get               |
| drs:migrationJob:getSwitchVipStatus         | Grants permission to query dual-VIP switchover result.                                  | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get               |

| Action                                       | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|----------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:batchDeleteJob              | Grants permission to batch delete tasks.                                   | write        | -                           | -                                                                                                                                                  | drs:migrationJob:delete |
| drs:migrationJob:batchOperateJob             | Grants permission to batch perform operations on tasks with specified IDs. | write        | -                           | -                                                                                                                                                  | drs:migrationJob:action |
| drs:migrationJob:getTaskLog                  | Grants permission to query migration logs.                                 | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:getLog |
| drs:migrationJob:getTuningParams             | Grants permission to query the value of a tuning parameter.                | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update |
| drs:migrationJob:checkAction                 | Grants permission to verify a task name.                                   | write        | -                           | -                                                                                                                                                  | drs:migrationJob:check  |
| drs:migrationJob:getUpdateObjectSavingStatus | Grants permission to obtain the progress of saving objects.                | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |

| Action                                     | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|--------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:getUserSelectedObjectInfo | Grants permission to query the synchronization mapping selected by a user. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |
| drs:migrationJob:cloneJobs                 | Grants permission to clone a MySQL synchronization task.                   | write        | -                           | -                                                                                                                                                  | drs:migrationJob:create |
| drs:migrationJob:getUserSetObjectInfo      | Grants permission to query synchronized object information.                | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |
| drs:migrationJob:jobAction                 | Grants permission to perform specific operations on a task.                | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:action |
| drs:migrationJob:jobUpdateAction           | Grants permission to start and stop tasks, capture, and replay.            | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update |
| drs:migrationJob:exportJobs                | Grants permission to export online migration tasks.                        | list         | -                           | -                                                                                                                                                  | drs:migrationJob:list   |

| Action                                    | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                   |
|-------------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:listJobs                 | Grants permission to query tasks of a tenant.                           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:migrationJob:list   |
| drs:migrationJob:getBatchTaskLog          | Grants permission to batch query migration logs.                        | list         | -                           | -                                                                                                                                                                                      | drs:migrationJob:getLog |
| drs:migrationJob:getCountdown             | Grants permission to query cloud service countdown information.         | list         | -                           | -                                                                                                                                                                                      | drs:migrationJob:get    |
| drs:migrationJob:getDrsJobByRdsInstanceId | Grants permission to query migration tasks related to RDS DB instances. | list         | -                           | -                                                                                                                                                                                      | drs:migrationJob:list   |
| drs:migrationJob:listJobs                 | Grants permission to query tasks of a tenant.                           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -                       |

| Action                                | Description                                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                            |
|---------------------------------------|--------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| drs:migrationJob:listReplayFaultsJobs | Grants permission to query the replay faults.                                                          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:replayFaultsJob:list         |
| drs:migrationJob:modifyColumnInfo     | Grants permission to modify the column information (column mapping and column filtering) of an object. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get             |
| drs:migrationJob:modifyCommonSetting  | Grants permission to update task configurations.                                                       | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:updateJobConfig |
| drs:migrationJob:modifyConflictPolicy | Grants permission to update the conflict policy of a synchronization task.                             | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:synchronizationJob:update    |
| drs:migrationJob:getJobs              | Grants permission to query online migration tasks.                                                     | list         | -                           | -                                                                                                                                                  | drs:migrationJob:list            |

| Action                                    | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                            |
|-------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| drs:migrationJob:getNodeNumByDDMInstance  | Grants permission to calculate the number of subtasks based on the number of DDM sharding nodes. | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get             |
| drs:migrationJob:modifyGroupAndStream     | Grants permission to enable or disable log reporting to LTS.                                     | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update          |
| drs:migrationJob:getPrecheckResult        | Grants permission to query the pre-check result of a migration task.                             | list         | -                           | -                                                                                                                                                  | drs:precheckJob:get              |
| drs:migrationJob:modifyIncreStartPosition | Grants permission to update the start point of an incremental task.                              | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:updateJobConfig |
| drs:migrationJob:getResourceInstances     | Grants permission to query resource instances and associated resources.                          | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get             |

| Action                                | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|---------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:modifyJob            | Grants permission to modify an online migration task.                               | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:modify |
| drs:migrationJob:modifySyncTypePolicy | Grants permission to update the synchronization type policy.                        | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:create |
| drs:migrationJob:getSubscribeNumber   | Grants permission to query the specifications of a yearly/monthly task.             | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get    |
| drs:migrationJob:operateJobByJobId    | Grants permission to perform operations on a task with a specified ID.              | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:action |
| drs:migrationJob:selectGroupAndStream | Grants permission to query whether the LTS service is enabled for the current task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get    |



| Action                            | Description                                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                            |
|-----------------------------------|---------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| drs:migrationJob:sendImportCheck  | Grants permission to upload Excel files.                                                    | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:update          |
| drs:migrationJob:switchVip        | Grants permission to perform dual-VIP switchover.                                           | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:action          |
| drs:migrationJob:updateDDLPolicy  | Grants permission to update the DDL filtering policy.                                       | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:updateDDLPolicy |
| drs:migrationJob:listProgressInfo | Grants permission to batch query the migration progress and incremental latency by task ID. | list         | -                           | -                                                                                                                                                  | drs:migrationJobs:getProgress    |

| Action                                  | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                   |
|-----------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:updateJobInfo          | Grants permission to update details about a task with a specified ID. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:migrationJob:update |
| drs:migrationJob:updateObjectInfo       | Grants permission to update database object selection information.    | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:update |
| drs:migrationJob:updateTuningParameters | Grants permission to modify tuning parameters.                        | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:update |
| drs:migrationJob:uploadDBObjectTemplate | Grants permission to upload the object import template.               | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | drs:migrationJob:update |

| Action                              | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                          | Alias                   |
|-------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:replayJob:downloadReport        | Grants permission to download files related to a workload replay task.        | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                     | drs:compareJob:list     |
| drs:replayJob:exportAbnormalSqlData | Grants permission to download abnormal SQL statements during workload replay. | list         | job                         | <ul style="list-style-type: none"> <li>• drs:netType</li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:supportFeature:get  |
| drs:migrationJob:resourceCheck      | Grants permission to check resources for creating an online migration task.   | write        | -                           | -                                                                                                                                                                                                                                                                      | drs:migrationJob:create |
| drs:migrationJob:skipPrecheck       | Grants permission to skip the pre-check.                                      | write        | -                           | -                                                                                                                                                                                                                                                                      | drs:migrationJob:check  |

| Action                               | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                  |
|--------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| drs:replayJob:exportSlowSqlData      | Grants permission to export SQL statements during workload replay.         | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |
| drs:replayJob:getAbnormalSqlData     | Grants permission to query abnormal SQL statements during workload replay. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |
| drs:replayJob:getAllSqlFile          | Grants permission to query full SQL files during workload replay.          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |
| drs:replayJob:getExecuteResultData   | Grants permission to query the result of a workload replay task.           | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |
| drs:replayJob:getExportSlowSqlStatus | Grants permission to query the export status of a workload replay file.    | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |

| Action                                  | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|-----------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| drs:replayJob:getReplayErrorTemplate    | Grants permission to query abnormal SQL templates.                                        | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get             |
| drs:replayJob:getReplayFile             | Grants permission to query files for a workload replay task.                              | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get             |
| drs:cloudDataGuardJob:getMonitoringData | Grants permission to query DR monitoring data based on the task ID.                       | list         | -                           | -                                                                                                                                                  | drs:disasterRecoveryJob:get        |
| drs:cloudDataGuardJob:batchSwitchover   | Grants permission to batch perform primary/standby switchover.                            | write        | -                           | -                                                                                                                                                  | drs:disasterRecoveryJob:switchover |
| drs:cloudDataGuardJob:listJobInfo       | Grants permission to query details about DR initialization objects in batches by task ID. | list         | -                           | -                                                                                                                                                  | drs:disasterRecoveryJob:get        |

| Action                                            | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias                            |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------|
| drs:cloudDataGuardJob:listRpoAndRto               | Grants permission to batch query RPO and RTO.                                                     | list         | -                           | -             | drs:dataGuardJob:list            |
| drs:cloudDataGuardJob:listStructProcess           | Grants permission to query the progress of DR initialization in batches by task ID.               | list         | -                           | -             | drs:disasterRecoveryJob:get      |
| drs:migrationJob:batchSetSmn                      | Grants permission to batch set alarm information.                                                 | write        | -                           | -             | drs:migrationJob:action          |
| drs:migrationJob:batchSetSpeedLimit               | Grants permission to batch set control flow.                                                      | write        | -                           | -             | drs:migrationJob:update          |
| drs:migrationJob:batchUpdateDefinerMigrateSetting | Grants permission to set whether to migrate Definers to the user in batches.                      | write        | -                           | -             | drs:migrationJob:updateJobConfig |
| drs:migrationJob:batchUpdateJobInfo               | Grants permission to modify task names or descriptions in batches and set exception notification. | write        | -                           | -             | drs:migrationJob:modify          |

| Action                                  | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                           |
|-----------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| drs:migrationJob:batchUpdateUserMigrate | Grants permission to set users and roles to be migrated in batches.             | write        | -                           | -                                                                                                                                                  | drs:migrationJob:modifyUserInfo |
| drs:migrationJob:changeSrcOrTargetPwd   | Grants permission to change the password of the source or destination database. | write        | -                           | -                                                                                                                                                  | drs:migrationJobs:update        |
| drs:migrationJob:setBatchSyncPolicy     | Grants permission to set synchronization policies in batches.                   | write        | -                           | -                                                                                                                                                  | drs:migrationJobs:add           |
| drs:replayJob:getReplayRecord           | Grants permission to query reports for a workload replay task.                  | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get          |
| drs:replayJob:getReplaySlowTemplate     | Grants permission to query slow SQL templates.                                  | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get          |

| Action                          | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                      |
|---------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| drs:replayJob:getSlowSqlData    | Grants permission to query slow SQL statements during workload replay. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | drs:supportFeature:get     |
| drs:replayJob:listReplayData    | Grants permission to query the statistics list during workload replay. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | drs:supportFeature:get     |
| drs:subscriptionJob:createJob   | Grants permission to create a data subscription task.                  | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | drs:subscriptionJob:create |
| drs:subscriptionJob:deleteJob   | Grants permission to delete a data subscription task.                  | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | drs:subscriptionJob:delete |
| drs:subscriptionJob:editJobInfo | Grants permission to edit subscription task information.               | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | drs:subscriptionJob:edit   |



| Action                                    | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                 |
|-------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| drs:subscriptionJob:getJobDetail          | Grants permission to query details about a data subscription task.   | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:subscriptionJob:get               |
| drs:subscriptionJob:getSubscriptionRecord | Grants permission to query detailed subscription content.            | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:subscriptionJob:get               |
| drs:subscriptionJob:jobAction             | Grants permission to perform operations on a data subscription task. | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:subscriptionJob:subscribe         |
| drs:configuration:getUserGuideInfo        | Grants permission to obtain user guide details.                      | list         | -                           | -                                                                                                                                                  | drs:userGuide:list                    |
| drs:configuration:modifyUserGuideInfo     | Grants permission to update the user guide.                          | write        | -                           | -                                                                                                                                                  | drs:userGuide:update                  |
| drs:subscriptionJob:updateConsumeTime     | Grants permission to modify the consumption time point.              | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:subscriptionJob:UpdateConsumeTime |

| Action                                           | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                      |
|--------------------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| drs:subscriptionJob:updateJob                    | Grants permission to modify a data subscription task.                                        | write        | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:subscriptionJob:update |
| drs:cloudDataGuardJob:getRdsInstanceCount        | Grants permission to query the number of RDS DB instances bound to a specified DDM instance. | list         | -                           | -                                                                                                                                                  | drs:dataGuardJob:list      |
| drs:configuration:getAvailableNodeType           | Grants permission to query available node specifications.                                    | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get       |
| drs:configuration:getAvailableZoneWithoutSellOut | Grants permission to query available AZs where node specifications are not sold out.         | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get       |
| drs:configuration:listAvailableZoneStatus        | Grants permission to query the AZ status.                                                    | list         | -                           | -                                                                                                                                                  | drs:migrationJob:get       |
| drs:configuration:listAvailableZone              | Grants permission to query available AZs.                                                    | list         | -                           | -                                                                                                                                                  | drs:configuration:list     |

| Action                               | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                   |
|--------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------|
| drs:migrationJob:listAvailableZone   | Grants permission to query AZs where specifications are not sold out. | list         | -                           | -                                                                                                              | drs:migrationJob:get    |
| drs:configuration:listResourcesByTag | Grants permission to query tasks by tag.                              | list         | -                           | -                                                                                                              | drs:tag:get             |
| drs::listDrivers                     | Grants permission to query drivers.                                   | list         | -                           | -                                                                                                              | drs:migrationJob:get    |
| drs::uploadDriver                    | Grants permission to upload drivers.                                  | write        | -                           | -                                                                                                              | drs:migrationJob:update |
| drs::deleteDriver                    | Grants permission to delete drivers.                                  | write        | -                           | -                                                                                                              | drs:migrationJob:delete |
| drs:migrationJob:syncDriver          | Grants permission to synchronize drivers.                             | write        | -                           | -                                                                                                              | drs:migrationJob:update |
| drs:configuration:modifyConfigInfo   | Grants permission to update task parameters.                          | write        | job                         | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | drs:migrationJob:modify |

| Action                                    | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                  |
|-------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| drs:configuration:getJobParameters        | Grants permission to query task parameter configuration list.          | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get   |
| drs:configuration:getJobParametersHistory | Grants permission to query the parameter change history of a task.     | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:migrationJob:get   |
| drs:replayJob:showReplayTimeScope         | Grants permission to query the time window for a workload replay task. | read         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |
| drs:replayJob:showReplayResults           | Grants permission to query the result data for a workload replay task. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |
| drs:replayJob:exportReport                | Grants permission to export reports for a workload replay task.        | read         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |

| Action                               | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                  |
|--------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| drs:replayJob:showReportExportStatus | Grants permission to query the export status of a workload replay report.    | read         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |
| drs:replayJob:showReportFileObsUris  | Grants permission to query the download address of a workload replay report. | list         | job                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | drs:supportFeature:get |

Each API of DRS usually supports one or more actions. [Table 3-117](#) lists the supported actions and dependencies.

**Table 3-117** Actions and dependencies supported by DRS APIs

| API                                             | Action                                 | Dependencies |
|-------------------------------------------------|----------------------------------------|--------------|
| DELETE /v3/{project_id}/jobs/batch-jobs         | drs:migrationJobAb:batchDeleteJobs     | -            |
| DELETE /v5/{project_id}/jdbc-drivers            | drs::deleteDriver                      | -            |
| DELETE /v5/{project_id}/jobs                    | drs:migrationJob:batchDeleteJob        | -            |
| DELETE /v5/{project_id}/jobs/{job_id}           | drs:migrationJob:deleteJob             | -            |
| GET /v3/{project_id}/jobs/{job_id}/get-src-user | drs:migrationJob:getSrcUsers           | -            |
| GET /v3/{project_id}/node-type                  | drs:configuration:getAvailableNodeType | -            |

| API                                                        | Action                                      | Dependencies |
|------------------------------------------------------------|---------------------------------------------|--------------|
| GET /v3/{project_id}/quotas                                | drs:configuration:getQuota                  | -            |
| GET /v5.1/{project_id}/jobs/{job_id}/db-object             | drs:migrationJob:getDbObjects               | -            |
| GET /v5/{project_id}/{resource_type}/{resource_id}/tags    | drs:configuration:getInstanceTag            | -            |
| GET /v5/{project_id}/{resource_type}/tags                  | drs:configuration:getProjectTags            | -            |
| GET /v5/{project_id}/batch-async-jobs                      | drs:migrationJob:listAsyncJobs              | -            |
| GET /v5/{project_id}/batch-async-jobs/{async_job_id}       | drs:migrationJob:listAsyncJobDetail         | -            |
| GET /v5/{project_id}/enterprise-projects                   | drs:configuration:listEPs                   | -            |
| GET /v5/{project_id}/jdbc-drivers                          | drs::listDrivers                            | -            |
| GET /v5/{project_id}/job/{job_id}/columns                  | drs:configuration:getColumnInfo             | -            |
| GET /v5/{project_id}/job/{job_id}/data-filtering/result    | drs:configuration:getDataTransformationData | -            |
| GET /v5/{project_id}/jobs                                  | drs:migrationJob:getJobList                 | -            |
| GET /v5/{project_id}/jobs/{job_id}                         | drs:migrationJob:getJobDetail               | -            |
| GET /v5/{project_id}/jobs/{job_id}/actions                 | drs:migrationJob:getAccess                  | -            |
| GET /v5/{project_id}/jobs/{job_id}/compare-policy          | drs:compareJob:getComparePolicy             | -            |
| GET /v5/{project_id}/jobs/{job_id}/configuration-histories | drs:configuration:getJobParametersHistory   | -            |
| GET /v5/{project_id}/jobs/{job_id}/configurations          | drs:configuration:getJobParameters          | -            |

| API                                                             | Action                                       | Dependencies |
|-----------------------------------------------------------------|----------------------------------------------|--------------|
| GET /v5/{project_id}/jobs/{job_id}/data-processing-rules        | drs:configuration:getDataTransformationInfo  | -            |
| GET /v5/{project_id}/jobs/{job_id}/data-processing-rules/result | drs:configuration:getDataTransformationInfo  | -            |
| GET /v5/{project_id}/jobs/{job_id}/db-object/template           | drs:migrationJob:downloadDBObjectTemplate    | -            |
| GET /v5/{project_id}/jobs/{job_id}/db-object/template/progress  | drs:migrationJob:getDBObjectTemplateProgress | -            |
| GET /v5/{project_id}/jobs/{job_id}/db-object/template/result    | drs:migrationJob:getDBObjectTemplateResult   | -            |
| GET /v5/{project_id}/jobs/{job_id}/db-objects                   | drs:migrationJob:getDbObjects                | -            |
| GET /v5/{project_id}/jobs/{job_id}/db-objects/collection-status | drs:migrationJob:getDBObjectCollectionStatus | -            |
| GET /v5/{project_id}/jobs/{job_id}/db-objects/saving-status     | drs:migrationJob:getUpdateObjectSavingStatus | -            |
| GET /v5/{project_id}/jobs/{job_id}/db-position                  | drs:migrationJob:checkAction                 | -            |
| GET /v5/{project_id}/jobs/{job_id}/dirty-data                   | drs:migrationJob:listReplayFaultsJobs        | -            |
| GET /v5/{project_id}/jobs/{job_id}/health-compare-jobs          | drs:compareJob:listHealthCompareJobs         | -            |
| GET /v5/{project_id}/jobs/{job_id}/increment-components-detail  | drs:migrationJob:getIncreComponentsDetails   | -            |
| GET /v5/{project_id}/jobs/{job_id}/metering                     | drs:migrationJob:getJobMeteringPrice         | -            |
| GET /v5/{project_id}/jobs/{job_id}/monitor-data                 | drs:cloudDataGuardJob:getDataGuardMonitor    | -            |

| API                                                     | Action                                       | Dependencies |
|---------------------------------------------------------|----------------------------------------------|--------------|
| GET /v5/{project_id}/jobs/{job_id}/object/support       | drs:migrationJob:getSupportObject            | -            |
| GET /v5/{project_id}/jobs/{job_id}/progress-data/{type} | drs:migrationJob:getObjectsCompareOverviewa  | -            |
| GET /v5/{project_id}/jobs/{resource_type}/{job_id}/tags | drs:configuration:getInstanceTag             | -            |
| GET /v5/{project_id}/jobs/{resource_type}/tags          | drs:configuration:getProjectTags             | -            |
| GET /v5/{project_id}/jobs/template                      | drs:migrationJob:downloadBatchCreateTemplate | -            |
| GET /v5/{project_id}/links                              | drs:configuration:listLinks                  | -            |
| POST /v3/{project_id}/available-zone                    | drs:migrationJob:listAvailableZone           | -            |
| POST /v3/{project_id}/jobs                              | drs:migrationJob:listJobs                    | -            |
| POST /v3/{project_id}/jobs/{job_id}/params              | drs:configuration:modifyDatabaseParams       | -            |
| POST /v3/{project_id}/jobs/{type}/batch-struct-detail   | drs:cloudDataGuardJob:listJobInfo            | -            |
| POST /v3/{project_id}/jobs/batch-connection             | drs:migrationJob:batchTestConnection         | -            |
| POST /v3/{project_id}/jobs/batch-creation               | drs:migrationJob:batchCreateJob              | -            |
| POST /v3/{project_id}/jobs/batch-detail                 | drs:migrationJob:listJobInfo                 | -            |
| POST /v3/{project_id}/jobs/batch-get-params             | drs:configuration:listDatabaseParams         | -            |
| POST /v3/{project_id}/jobs/batch-pause-task             | drs:migrationJob:batchPauseJob               | -            |



| API                                                 | Action                                            | Dependencies |
|-----------------------------------------------------|---------------------------------------------------|--------------|
| POST /v3/{project_id}/jobs/batch-precheck           | drs:migrationJob:batchPreCheckJob                 | -            |
| POST /v3/{project_id}/jobs/batch-precheck-result    | drs:migrationJob:listPrecheckResult               | -            |
| POST /v3/{project_id}/jobs/batch-progress           | drs:migrationJob:listProgressInfo                 | -            |
| POST /v3/{project_id}/jobs/batch-replace-definer    | drs:migrationJob:batchUpdateDefinerMigrateSetting | -            |
| POST /v3/{project_id}/jobs/batch-retry-task         | drs:migrationJob:batchRetryJob                    | -            |
| POST /v3/{project_id}/jobs/batch-rpo-and-rto        | drs:cloudDataGuardJob:listRpoAndRto               | -            |
| POST /v3/{project_id}/jobs/batch-set-smn            | drs:migrationJob:batchSetSmn                      | -            |
| POST /v3/{project_id}/jobs/batch-starting           | drs:migrationJob:batchStartJob                    | -            |
| POST /v3/{project_id}/jobs/batch-status             | drs:migrationJob:listJobStatus                    | -            |
| POST /v3/{project_id}/jobs/batch-struct-process     | drs:cloudDataGuardJob:listStructProcess           | -            |
| POST /v3/{project_id}/jobs/batch-switchover         | drs:cloudDataGuardJob:batchSwitchover             | -            |
| POST /v3/{project_id}/jobs/batch-sync-policy        | drs:migrationJob:setBatchSyncPolicy               | -            |
| POST /v3/{project_id}/jobs/batch-transformation     | drs:migrationJob:batchSetTransformation           | -            |
| POST /v3/{project_id}/jobs/cluster/batch-connection | drs:migrationJob:batchTestClusterConnection       | -            |
| POST /v3/{project_id}/jobs/create-compare-task      | drs:compareJob:createJob                          | -            |

| API                                                             | Action                                        | Dependencies |
|-----------------------------------------------------------------|-----------------------------------------------|--------------|
| POST /v3/{project_id}/jobs/disaster-recovery-monitoring-data    | drs:cloudDataGuardJob:getMonitoringData       | -            |
| POST /v3/{project_id}/jobs/query-compare-result                 | drs:compareJob:getCompareResult               | -            |
| POST /v5.1/{project_id}/jobs/{job_id}/db-objects/collect        | drs:migrationJob:getDbObjectsCollectAsync     | -            |
| POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create | drs:configuration:addTag                      | -            |
| POST /v5/{project_id}/{resource_type}/{resource_id}/tags/delete | drs:configuration:deleteTag                   | -            |
| POST /v5/{project_id}/{resource_type}/resource-instances/count  | drs:configuration:listResourcesByTag          | -            |
| POST /v5/{project_id}/{resource_type}/resource-instances/filter | drs:configuration:listResourcesByTag          | -            |
| POST /v5/{project_id}/batch-async-jobs/{async_job_id}/commit    | drs:migrationJob:asyncBatchCreateJobByAsyncId | -            |
| POST /v5/{project_id}/jdbc-driver                               | drs::uploadDriver                             | -            |
| POST /v5/{project_id}/job/{job_id}/columns/collect              | drs:configuration:getColumnInfo               | -            |
| POST /v5/{project_id}/job/{job_id}/data-filtering/check         | drs:configuration:checkDataTransformationInfo | -            |
| POST /v5/{project_id}/jobs                                      | drs:migrationJob:createJobs                   | -            |
| POST /v5/{project_id}/jobs/{job_id}/action                      | drs:migrationJob:operateJobByJobId            | -            |
| POST /v5/{project_id}/jobs/{job_id}/collect-db-position         | drs:migrationJob:checkAction                  | -            |
| POST /v5/{project_id}/jobs/{job_id}/db-object/template          | drs:migrationJob:uploadDbObjectTemplate       | -            |

| API                                                             | Action                                     | Dependencies |
|-----------------------------------------------------------------|--------------------------------------------|--------------|
| POST /v5/{project_id}/jobs/{job_id}/db-objects/collect          | drs:migrationJob:getDbObjectsCollectAsync  | -            |
| POST /v5/{project_id}/jobs/{job_id}/object-mappings             | drs:migrationJob:getUserSelectedObjectInfo | -            |
| POST /v5/{project_id}/jobs/{job_id}/operation-statistics/export | drs:migrationJob:getOperationInfo          | -            |
| POST /v5/{project_id}/jobs/{job_id}/stop                        | drs:migrationJob:deleteJob                 | -            |
| POST /v5/{project_id}/jobs/{resource_type}/{job_id}/tags/action | drs:configuration:batchReplaceTags         | -            |
| POST /v5/{project_id}/jobs/action                               | drs:migrationJob:batchOperateJob           | -            |
| POST /v5/{project_id}/jobs/batch-async-create                   | drs:migrationJob:asyncBatchSaveJob         | -            |
| POST /v5/{project_id}/jobs/batch-stop                           | drs:migrationJob:deleteJob                 | -            |
| POST /v5/{project_id}/jobs/clone                                | drs:migrationJob:cloneJobs                 | -            |
| POST /v5/{project_id}/jobs/name-validation                      | drs:migrationJob:checkAction               | -            |
| POST /v5/{project_id}/jobs/template                             | drs:migrationJob:importBatchCreateJobs     | -            |
| PUT /v3/{project_id}/job/{job_id}/tuning-params/modify-params   | drs:migrationJob:updateTuningParams        | -            |
| PUT /v3/{project_id}/jobs/batch-limit-speed                     | drs:migrationJob:batchSetSpeedLimit        | -            |
| PUT /v3/{project_id}/jobs/batch-modification                    | drs:migrationJob:batchUpdateJobInfo        | -            |
| PUT /v3/{project_id}/jobs/batch-modify-pwd                      | drs:migrationJob:changeSrcOrTargetPwd      | -            |

| API                                                      | Action                                        | Dependencies |
|----------------------------------------------------------|-----------------------------------------------|--------------|
| PUT /v3/{project_id}/jobs/batch-select-objects           | drs:migrationJob:selectDatabaseObject         | -            |
| PUT /v3/{project_id}/jobs/batch-update-user              | drs:migrationJob:batchUpdateUserMigrate       | -            |
| PUT /v5/{project_id}/batch-async-jobs/{async_job_id}     | drs:migrationJob:asyncBatchUpdateJobByAsyncId | -            |
| PUT /v5/{project_id}/jobs/{job_id}                       | drs:migrationJob:updateJobInfo                | -            |
| PUT /v5/{project_id}/jobs/{job_id}/data-processing-rules | drs:configuration:addDataTransformationInfo   | -            |
| PUT /v5/{project_id}/jobs/{job_id}/modify-configuration  | drs:configuration:modifyConfiguration         | -            |
| PUT /v5/{project_id}/jobs/{job_id}/start-position        | drs:migrationJob:modifyIncrementStartPosition | -            |
| PUT /v5/{project_id}/jobs/{job_id}/update-jdbc-driver    | drs:migrationJob:syncDriver                   | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-118](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

**Table 3-118** Resource types supported by DRS

| Resource Type | URN                                    |
|---------------|----------------------------------------|
| job           | drs:<region>:<account-id>:job:<job-id> |

## Conditions

DRS does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.6.5 TaurusDB

IAM provides system-defined policies to define common actions supported by cloud services. You can also create custom policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom policy, see [Creating a Custom Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in a policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource type defined by TaurusDB, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.

- If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
- If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
- If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by TaurusDB, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in custom policy statements for TaurusDB.

**Table 3-119** Actions supported by TaurusDB

| Action                                      | Description                                                              | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                                                          |
|---------------------------------------------|--------------------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:backup:modifyPolicy         | Grants permission to configure an automated backup policy.               | Permission management | -                           | <a href="#">gaussdbformysql:ReplicationTargetRegion</a>                                                                                        | <ul style="list-style-type: none"> <li>gaussdb:instance:modifyBackupPolicy</li> </ul>                          |
| gaussdbformysql:param:delete                | Grants permission to delete a parameter template.                        | Permission management | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:delete</li> </ul>                                         |
| gaussdbformysql:instance:switchover         | Grants permission to promote a read replica to primary.                  | Permission management | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> <li>gaussdb:instance:switchover</li> </ul> |
| gaussdbformysql:htapInstance:createDataSync | Grants permission to create a data synchronization task for an instance. | Write                 | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:htapInstance:createDataSync</li> </ul>                          |

| Action                                   | Description                                                    | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                |
|------------------------------------------|----------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| gaussdbformysql:auditlog:list            | Grants permission to query audit logs.                         | List                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> </ul>            |
| gaussdbformysql:autoscaling:createPolicy | Grants permission to configure auto scaling.                   | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:autoscaling:createPolicy</li> </ul> |
| gaussdbformysql:autoscaling:modifyPolicy | Grants permission to configure an auto scaling policy.         | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:serverless:modifyPolicy</li> </ul>  |
| gaussdbformysql:autoscaling:listHistory  | Grants permission to query historical records of auto scaling. | List                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:autoscaling:list</li> </ul>         |
| gaussdbformysql:autoscaling:listPolicy   | Grants permission to query auto scaling policies.              | Read                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:autoscaling:list</li> </ul>         |
| gaussdbformysql:backup:create            | Grants permission to create a manual backup.                   | Write                 | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:backup:create</li> </ul>            |
| gaussdbformysql:backup:delete            | Grants permission to delete a backup.                          | Write                 | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:backup:delete</li> </ul>            |

| Action                                | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                      |
|---------------------------------------|--------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:backup:getRestoreTime | Grants permission to query the restoration time range. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> <li>• gaussdb:backup:list</li> </ul>   |
| gaussdbformysql:backup:list           | Grants permission to query backups.                    | List         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> <li>• gaussdb:backup:list</li> </ul>   |
| gaussdbformysql:backup:listPolicy     | Grants permission to query backup policies.            | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:backup:list</li> </ul>                                    |
| gaussdbformysql:database:create       | Grants permission to create a database.                | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:database:create</li> </ul>                                |
| gaussdbformysql:database:delete       | Grants permission to delete a database.                | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:database:delete</li> </ul>                                |
| gaussdbformysql:database:list         | Grants permission to query databases.                  | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> <li>• gaussdb:database:list</li> </ul> |



| Action                                                  | Description                                                            | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                 |
|---------------------------------------------------------|------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| gaussdbformysql:database:modify                         | Grants permission to modify database information.                      | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:database:modify</li> </ul>           |
| gaussdbformysql:user:modifyHost                         | Grants permission to change a host IP address.                         | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:modify</li> </ul>               |
| gaussdbformysql:proxy:queryElb                          | Grants permission to query ELB information of a proxy instance.        | Read                  | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:elb:query</li> </ul>                 |
| gaussdbformysql:instance:getSecondLevelMonitoringConfig | Grants permission to query the configuration of Monitoring by Seconds. | Read                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> </ul>             |
| gaussdbformysql:htapInstance:bindPublicIp               | Grants permission to bind an EIP to an HTAP instance.                  | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:bindPublicIp</li> </ul> |
| gaussdbformysql:htapInstance:create                     | Grants permission to create an HTAP instance.                          | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:create</li> </ul>       |

| Action                                       | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                   |
|----------------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| gaussdbformysql:htapInstance:delete          | Grants permission to delete an HTAP instance.                                                 | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:delete</li> </ul>         |
| gaussdbformysql:htapInstance:deleteDataSync  | Grants permission to disable data synchronization between an HTAP instance and a DB instance. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:deleteDataSync</li> </ul> |
| gaussdbformysql:htapInstance:listDatabases   | Grants permission to query databases of an HTAP instance.                                     | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>           |
| gaussdbformysql:htapInstance:listDbParameter | Grants permission to query database parameters of an HTAP instance.                           | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>           |
| gaussdbformysql:htapInstance:getReplication  | Grants permission to query data synchronization information of an HTAP instance.              | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>           |

| Action                                            | Description                                                                         | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                   |
|---------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| gaussdbformysql:htapInstance:getReplicationConfig | Grants permission to query data synchronization configurations of an HTAP instance. | Read                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>           |
| gaussdbformysql:htapInstance:getTask              | Grants permission to query task details of an HTAP instance.                        | Read                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>           |
| gaussdbformysql:htapInstance:getTaskList          | Grants permission to query task records of an HTAP instance.                        | List                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>           |
| gaussdbformysql:htapInstance:list                 | Grants permission to query HTAP instances.                                          | List                  | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>           |
| gaussdbformysql:htapInstance:modifyDataSync       | Grants permission to modify a comparison task of an HTAP instance.                  | Permission management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:modifyDataSync</li> </ul> |
| gaussdbformysql:htapInstance:modifyPassword       | Grants permission to change the password of an HTAP instance database.              | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:modifyPassword</li> </ul> |

| Action                                         | Description                                                          | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                      |
|------------------------------------------------|----------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| gaussdbformysql:htapInstance:modifySpec        | Grants permission to change specifications of an HTAP instance.      | Permission management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:modifySpec</li> </ul>        |
| gaussdbformysql:htapInstance:modifyStorageSize | Grants permission to scale up storage of an HTAP instance.           | Permission management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:modifyStorageSize</li> </ul> |
| gaussdbformysql:htapInstance:restart           | Grants permission to reboot an HTAP instance.                        | Permission management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:restart</li> </ul>           |
| gaussdbformysql:htapInstance:tablesConfigCheck | Grants permission to check table configurations of an HTAP instance. | List                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>              |
| gaussdbformysql:htapInstance:unbindPublicIp    | Grants permission to unbind an EIP from an HTAP instance.            | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:unbindPublicIp</li> </ul>    |
| gaussdbformysql:htapInstance:get               | Grants permission to query HTAP instance details.                    | Read                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>              |

| Action                                     | Description                                                                    | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                            |
|--------------------------------------------|--------------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:htapInstance:createUser    | Grants permission to create a database user for an HTAP instance.              | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:user:create</li> </ul>       |
| gaussdbformysql:htapInstance:deleteUser    | Grants permission to delete a database user of an HTAP instance.               | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:delete</li> </ul>                                          |
| gaussdbformysql:htapInstance:grantUser     | Grants permission to authorize database user permissions for an HTAP instance. | Permission management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:grantPrivilege</li> </ul>                                  |
| gaussdbformysql:htapInstance:listUser      | Grants permission to query database users of an HTAP instance.                 | List                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>                                    |
| gaussdbformysql:htapInstance:dbConfigCheck | Grants permission to check database configurations of an HTAP instance.        | Read                  | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:htapInstance:list</li> </ul>                                    |
| gaussdbformysql:instance:addReadOnlyNodes  | Grants permission to add read replicas.                                        | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:addNodes</li> </ul> |

| Action                                        | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                     | Alias                                                                                                          |
|-----------------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:instance:create               | Grants permission to create a DB instance.                    | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">gaussdbformysql:FlavorType</a></li> <li>• <a href="#">gaussdbformysql:SubnetId</a></li> <li>• <a href="#">gaussdbformysql:VpcId</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:create</li> <li>• gaussdb:instance:modify</li> </ul> |
| gaussdbformysql:instance:delete               | Grants permission to delete a DB instance.                    | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• gaussdb:instance:delete</li> </ul>                                    |
| gaussdbformysql:instance:deleteRecycleBin     | Grants permission to delete table records in the recycle bin. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> </ul>                                    |
| gaussdbformysql:instance:deleteSqlFilterRules | Grants permission to delete SQL throttling rules.             | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• gaussdb:parameter:modify</li> </ul>                                   |
| gaussdbformysql:instance:get                  | Grants permission to query DB instance details.               | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                                                                                                                                | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> </ul>                                      |

| Action                                      | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| gaussdbformysql:instance:getDcc             | Grants permission to query the details about a dedicated resource pool. | Read         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:instance:getPublicIp        | Grants permission to obtain an EIP.                                     | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:instance:getSqlFilterRule   | Grants permission to query SQL throttling rules.                        | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:parameter:list</li> </ul>                            |
| gaussdbformysql:instance:getSqlFilterStatus | Grants permission to query whether SQL throttling is enabled.           | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:parameter:list</li> </ul>                            |
| gaussdbformysql:instance:killProcess        | Grants permission to kill sessions.                                     | Write        | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:tag:list</li> </ul>                                  |
| gaussdbformysql:instance:list               | Grants permission to query DB instances.                                | List         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:proxy:list                  | Grants permission to query proxy instances.                             | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> <li>gaussdb:proxy:list</li> </ul> |

| Action                               | Description                                                   | Access Level          | Resource Type (*: required) | Condition Key | Alias                                                                                               |
|--------------------------------------|---------------------------------------------------------------|-----------------------|-----------------------------|---------------|-----------------------------------------------------------------------------------------------------|
| gaussdbformysql:proxy:listSpec       | Grants permission to query proxy instance specifications.     | List                  | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> <li>gaussdb:proxy:list</li> </ul> |
| gaussdbformysql:instance:listDcc     | Grants permission to query dedicated resources.               | List                  | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:instance:listDccSpec | Grants permission to query dedicated resource specifications. | List                  | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:instance:listEngine  | Grants permission to query the DB engine information.         | List                  | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:instance:listProcess | Grants permission to query process sessions.                  | List                  | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:tag:list</li> </ul>                                  |
| gaussdbformysql:instance:listSpec    | Grants permission to query specifications.                    | List                  | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:instance:metering    | Grants permission to query metering information.              | List                  | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:metering</li> </ul>                         |
| gaussdbformysql:instance:modify      | Grants permission to modify instance information.             | Permission management | -                           | -             | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> </ul>                           |



| Action                                                  | Description                                                                 | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                                           |
|---------------------------------------------------------|-----------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:auditlog:operate                        | Grants permission to enable or disable audit log.                           | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifyTraceSQLPolicy</li> </ul>    |
| gaussdbformysql:instance:bindPublicIp                   | Grants permission to bind an EIP to a DB instance.                          | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:bindPublicIp</li> </ul>            |
| gaussdbformysql:instance:deleteReadOnlyNodes            | Grants permission to delete a read replica.                                 | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:deleteNodes</li> </ul>             |
| gaussdbformysql:instance:modifyVip                      | Grants permission to change a private IP address.                           | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifyVip</li> </ul>               |
| gaussdbformysql:instance:modifyMaintenanceWindow        | Grants permission to change the maintenance window of a DB instance.        | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifyMaintenanceWindow</li> </ul> |
| gaussdbformysql:instance:modifySecondLevelMonitorPolicy | Grants permission to change the collection period of Monitoring by Seconds. | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifyMonitorPolicy</li> </ul>     |

| Action                                       | Description                                                         | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                                       |
|----------------------------------------------|---------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:instance:modifyPassword      | Grants permission to change a DB instance password.                 | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifyPassword</li> </ul>      |
| gaussdbformysql:instance:modifyPort          | Grants permission to change a DB instance port.                     | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifyPort</li> </ul>          |
| gaussdbformysql:instance:modifySecurityGroup | Grants permission to change a security group.                       | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifySecurityGroup</li> </ul> |
| gaussdbformysql:instance:modifySSL           | Grants permission to enable or disable SSL.                         | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifySSL</li> </ul>           |
| gaussdbformysql:instance:modifyStorageSize   | Grants permission to scale up or down the storage of a DB instance. | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifyStorageSize</li> </ul>   |

| Action                                            | Description                                                             | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                                            |
|---------------------------------------------------|-------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:instance:modifySwitchoverPriority | Grants permission to change the failover priority of a read replica.    | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifySwitchoverPriority</li> </ul> |
| gaussdbformysql:instance:rename                   | Grants permission to change a DB instance name.                         | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:rename</li> </ul>                   |
| gaussdbformysql:instance:unbindPublicIp           | Grants permission to unbind an EIP from a DB instance.                  | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:unbindPublicIp</li> </ul>           |
| gaussdbformysql:instance:upgrade                  | Grants permission to upgrade the kernel version of a DB instance.       | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:upgrade</li> </ul>                  |
| gaussdbformysql:instance:createDns                | Grants permission to apply for a private domain name for a DB instance. | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:createDns</li> </ul>                                                   |
| gaussdbformysql:instance:modifyDns                | Grants permission to change the private domain name of a DB instance.   | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyDns</li> </ul>                                                   |

| Action                          | Description                                                                | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                               |
|---------------------------------|----------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:user:create     | Grants permission to create a database account.                            | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:user:create</li> </ul>          |
| gaussdbformysql:proxy:addNodes  | Grants permission to add proxy nodes.                                      | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:addNodes</li> </ul>  |
| gaussdbformysql:proxy:changeElb | Grants permission to modify ELB information of a proxy instance.           | Permission management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:changeElb</li> </ul> |
| gaussdbformysql:proxy:createDns | Grants permission to apply for a private domain name for a proxy instance. | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:createDns</li> </ul> |
| gaussdbformysql:proxy:create    | Grants permission to create a proxy instance.                              | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:create</li> </ul>    |
| gaussdbformysql:proxy:delete    | Grants permission to delete a proxy instance.                              | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:delete</li> </ul>    |

| Action                             | Description                                                             | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                                  |
|------------------------------------|-------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:proxy:modifyAccess | Grants the access control permission to a proxy instance.               | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:modifyAccess</li> </ul> |
| gaussdbformysql:proxy:modifyIp     | Grants permission to change the IP address of a proxy instance.         | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:modifyIp</li> </ul>     |
| gaussdbformysql:proxy:modifySpec   | Grants permission to change specifications of a proxy instance.         | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:modifySpec</li> </ul>   |
| gaussdbformysql:proxy:modifyWeight | Grants permission to change read weights of nodes for a proxy instance. | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:modifyWeight</li> </ul> |
| gaussdbformysql:proxy:rename       | Grants permission to rename a proxy instance.                           | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:rename</li> </ul>       |
| gaussdbformysql:proxy:restart      | Grants permission to reboot a proxy instance.                           | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:restart</li> </ul>      |

| Action                                         | Description                                                               | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                                              |
|------------------------------------------------|---------------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:proxy:switchConnectionPoolType | Grants permission to change the connection pool type of a proxy instance. | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:switchConnectionPoolType</li> </ul> |
| gaussdbformysql:proxy:updateConfigurations     | Grants permission to modify the kernel parameters of a proxy instance.    | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:updateConfigurations</li> </ul>     |
| gaussdbformysql:instance:modifyRecycleBin      | Grants permission to modify a recycling policy.                           | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> </ul>                                                        |
| gaussdbformysql:instance:modifySpec            | Grants permission to change DB instance specifications.                   | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> <li>• gaussdb:instance:modifySpec</li> </ul>                 |
|                                                |                                                                           |                       | -                           | <a href="#">gaussdbformysql:FlavorType</a>                                                                                                         |                                                                                                                                    |
| gaussdbformysql:instance:restart               | Grants permission to reboot a DB instance.                                | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:restart</li> </ul>                                                       |

| Action                                      | Description                                                                  | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                             |
|---------------------------------------------|------------------------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| gaussdbformysql:instance:restoreInPlace     | Grants permission to restore data to an existing DB instance using a backup. | Permission_management | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:instance:restoreInPlace</li> </ul> |
| gaussdbformysql:instance:setRecycleBin      | Grants permission to configure a recycling policy.                           | Permission_management | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> </ul>         |
| gaussdbformysql:instance:setSqlFilterRules  | Grants permission to configure SQL throttling rules.                         | Write                 | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:param:modify</li> </ul>            |
| gaussdbformysql:instance:setSqlFilterStatus | Grants permission to enable or disable SQL throttling.                       | Permission_management | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:param:modify</li> </ul>            |
| gaussdbformysql:instance:tableRestore       | Grants permission to restore tables to a point in time.                      | Permission_management | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:instance:tableRestore</li> </ul>   |
| gaussdbformysql:tag:deal                    | Grants permission to add or delete resource tags.                            | Write                 | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:instance:dealTag</li> </ul>        |
|                                             |                                                                              |                       | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              |                                                                                   |

| Action                              | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                                             |
|-------------------------------------|-------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| gaussdbformysql:log:createLtsConfig | Grants permission to create LTS configurations. | Write        | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:log:createLtsConfig</li> </ul>                     |
| gaussdbformysql:log:deleteLtsConfig | Grants permission to delete LTS configurations. | Write        | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:log:deleteLtsConfig</li> </ul>                     |
| gaussdbformysql:log:getErrorLogs    | Grants permission to query error logs.          | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:log:list</li> </ul>                                |
| gaussdbformysql:log:getSlowLogs     | Grants permission to query slow query logs.     | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:log:list</li> <li>gaussdb:instance:list</li> </ul> |
| gaussdbformysql:log:list            | Grants permission to query log information.     | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:log:list</li> </ul>                                |
| gaussdbformysql:log:listLtsConfig   | Grants permission to query LTS configurations.  | List         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:log:listLtsConfig</li> </ul>                       |
| gaussdbformysql:log:operate         | Grants permission to operate logs.              | Write        | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:tag:list</li> </ul>                                |



| Action                                        | Description                                                    | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                     |
|-----------------------------------------------|----------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| gaussdbformysql:log:operateBinLog             | Grants permission to enable or disable Binlog.                 | Write                 | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:tag:list</li> </ul>        |
| gaussdbformysql:log:setSlowLogSensitiveStatus | Grants permission to enable or disable Show Original Log.      | Permission_management | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:instance:modify</li> </ul> |
| gaussdbformysql:param:apply                   | Grants permission to apply a parameter template.               | Permission_management | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:apply</li> </ul>     |
| gaussdbformysql:param:create                  | Grants permission to create a parameter template.              | Write                 | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:create</li> </ul>    |
| gaussdbformysql:param:get                     | Grants permission to query parameter template details.         | Read                  | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:list</li> </ul>      |
| gaussdbformysql:param:getParameter            | Grants permission to query parameter details of a DB instance. | Read                  | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:param:list</li> </ul>      |
| gaussdbformysql:param:list                    | Grants permission to query parameter templates.                | List                  | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:list</li> </ul>      |

| Action                                       | Description                                                                        | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                                  |
|----------------------------------------------|------------------------------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| gaussdbformysql:param:reset                  | Grants permission to reset a parameter template.                                   | Write                 | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:modify</li> </ul>                 |
| gaussdbformysql:param:save                   | Grants permission to save a parameter template.                                    | Write                 | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:modify</li> </ul>                 |
| gaussdbformysql:param:update                 | Grants permission to modify parameters in a parameter template.                    | Write                 | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>gaussdb:param:modify</li> </ul>                 |
| gaussdbformysql:proxy:modifyConsistency      | Grants permission to change session consistency of a proxy instance.               | Permission_management | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:proxy:modifyConsistency</li> </ul>      |
| gaussdbformysql:proxy:modifyTransactionSplit | Grants permission to enable or disable transaction splitting for a proxy instance. | Permission_management | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:proxy:modifyTransactionSplit</li> </ul> |
| gaussdbformysql:proxy:queryConfigurations    | Grants permission to query the kernel parameters of a proxy instance.              | Read                  | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>gaussdb:proxy:queryConfigurations</li> </ul>    |

| Action                        | Description                                                          | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                 |
|-------------------------------|----------------------------------------------------------------------|-----------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| gaussdbformysql:proxy:upgrade | Grants permission to upgrade the kernel version of a proxy instance. | Permission_management | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:upgrade</li> </ul>                             |
| gaussdbformysql:quota:list    | Grants permission to query quotas.                                   | Read                  | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:quota:modify  | Grants permission to modify quotas.                                  | Write                 | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:quota:modify</li> </ul>                              |
| gaussdbformysql:tag:delete    | Grants permission to delete a tag.                                   | Write                 | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modify</li> </ul>                           |
| gaussdbformysql:tag:list      | Grants permission to query tags.                                     | List                  | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> <li>• gaussdb:tag:list</li> </ul> |
| gaussdbformysql:task:delete   | Grants permission to delete a task record.                           | Write                 | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:instance:delete</li> </ul>                           |
| gaussdbformysql:task:get      | Grants permission to query the execution progress of a task.         | Read                  | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> </ul>                             |
| gaussdbformysql:task:list     | Grants permission to query task records.                             | List                  | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• gaussdb:instance:list</li> </ul>                             |

| Action                               | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                            |
|--------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| gaussdbformysql:user:delete          | Grants permission to delete a database account.                | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:delete</li> </ul>          |
| gaussdbformysql:user:grantPrivilege  | Grants permission to change permissions of a database user.    | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:grantPrivilege</li> </ul>  |
| gaussdbformysql:user:list            | Grants permission to query database users.                     | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:list</li> </ul>            |
| gaussdbformysql:user:modify          | Grants permission to query the description of a database user. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:modify</li> </ul>          |
| gaussdbformysql:user:revokePrivilege | Grants permission to delete permissions of a database user.    | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:revokePrivilege</li> </ul> |
| gaussdbformysql:user:updatePassword  | Grants permission to change the password of a database user.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:user:modify</li> </ul>          |

| Action                                | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                             |
|---------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| gaussdbformysql:backup:encrypt        | Grants permission to enable or disable encrypted backup for a DB instance. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:backup:encrypt</li> </ul>        |
| gaussdbformysql:proxy:modifyPort      | Grants permission to change the port of a proxy instance.                  | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:modifyPort</li> </ul>      |
| gaussdbformysql:proxy:modifyRouteMode | Grants permission to configure a routing policy for a proxy instance.      | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:modifyRouteMode</li> </ul> |
| gaussdbformysql:proxy:modifyDns       | Grants permission to change the private domain name of a proxy instance.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:modifyDns</li> </ul>       |
| gaussdbformysql:proxy:deleteDns       | Grants permission to delete the private domain name of a proxy instance.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:deleteDns</li> </ul>       |
| gaussdbformysql:proxy:modifySSL       | Grants permission to enable or disable SSL for a proxy instance.           | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:modifySSL</li> </ul>       |

| Action                                             | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                                 |
|----------------------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| gaussdbformysql:proxy:modifySlowLog                | Grants permission to enable or disable slow query log reporting for a proxy instance. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:modifySlowLog</li> </ul>                                       |
| gaussdbformysql:proxy:modifyAlt                    | Grants permission to enable or disable ALT for a proxy instance.                      | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:modifyAlt</li> </ul>                                           |
| gaussdbformysql:instance:listProcesses             | Grants permission to query user session threads on an instance node.                  | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:listProcesses</li> </ul>                                    |
| gaussdbformysql:instance:deleteProcesses           | Grants permission to terminate user session threads on an instance node.              | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:deleteProcesses</li> </ul>                                  |
| gaussdbformysql:proxy:deleteNodes                  | Grants permission to delete proxy nodes.                                              | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyProxy</li> <li>• gaussdb:proxy:deleteNodes</li> </ul> |
| gaussdbformysql:serverless:getComputeAbilityPolicy | Grants permission to query a serverless compute policy.                               | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:serverless:getComputeAbilityPolicy</li> </ul>                        |

| Action                                                | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                             |
|-------------------------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| gaussdbformysql:serverless:updateComputeAbilityPolicy | Grants permission to configure a serverless compute policy.                        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:serverless:updateComputeAbilityPolicy</li> </ul> |
| gaussdbformysql:serverless:getScalingPolicy           | Grants permission to query custom scale-up policies of a serverless instance.      | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:serverless:getScalingPolicy</li> </ul>           |
| gaussdbformysql:serverless:updateScalingPolicy        | Grants permission to configure custom scale-up policies for a serverless instance. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:serverless:updateScalingPolicy</li> </ul>        |
| gaussdbformysql:coldTable:operate                     | Grants permission to separate hot and cold data.                                   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:coldTable:operate</li> </ul>                     |
| gaussdbformysql:coldTable:query                       | Grants permission to query hot and cold data separation.                           | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:coldTable:query</li> </ul>                       |
| gaussdbformysql:instance:modifyIp                     | Grants permission to change the private IP address for read of a read replica.     | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:instance:modifyIp</li> </ul>                     |

| Action                                 | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                              |
|----------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| gaussdbformysql:proxy:modifyBinlogPull | Grants permission to enable or disable binlog pull for a proxy instance.    | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:modifyBinlogPull</li> </ul> |
| gaussdbformysql:proxy:bindEip          | Grants permission to bind an EIP to or unbind an EIP from a proxy instance. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• gaussdb:proxy:bindEip</li> </ul>          |

Each API of TaurusDB usually supports one or more actions. [Table 3-120](#) lists the supported actions and dependencies.

**Table 3-120** Actions and dependencies supported by TaurusDB APIs

| API                                                             | Action                                       | Dependency |
|-----------------------------------------------------------------|----------------------------------------------|------------|
| GET /v3/{project_id}/datastores/{database_name}                 | gaussdbformysql:instance:listEngine          | -          |
| GET /v3/{project_id}/flavors/{database_name}                    | gaussdbformysql:instance:listSpec            | -          |
| POST /v3/{project_id}/instances                                 | gaussdbformysql:instance:create              | -          |
| POST /v3/{project_id}/instances/{instance_id}/restart           | gaussdbformysql:instance:restart             | -          |
| DELETE /v3/{project_id}/instances/{instance_id}                 | gaussdbformysql:instance:delete              | -          |
| POST /v3/{project_id}/instances/{instance_id}/nodes/enlarge     | gaussdbformysql:instance:addReadOnlyNodes    | -          |
| DELETE /v3/{project_id}/instances/{instance_id}/nodes/{node_id} | gaussdbformysql:instance:deleteReadOnlyNodes | -          |



| API                                                                   | Action                                       | Dependenc<br>y |
|-----------------------------------------------------------------------|----------------------------------------------|----------------|
| POST /v3/{project_id}/instances/{instance_id}/volume/extend           | gaussdbformysql:instance:modifyStorageSize   | -              |
| PUT /v3/{project_id}/instances/{instance_id}/backups/policy/update    | gaussdbformysql:backup:modifyPolicy          | -              |
| PUT /v3/{project_id}/instances/{instance_id}/name                     | gaussdbformysql:instance:rename              | -              |
| POST /v3/{project_id}/instances/{instance_id}/password                | gaussdbformysql:instance:modifyPassword      | -              |
| POST /v3/{project_id}/instances/{instance_id}/action                  | gaussdbformysql:instance:modifySpec          | -              |
| GET /v3/{project_id}/dedicated-resources                              | gaussdbformysql:instance:listDcc             | -              |
| GET /v3/{project_id}/dedicated-resource/{dedicated_resource_id}       | gaussdbformysql:instance:getDcc              | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy                   | gaussdbformysql:proxy:create                 | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/proxy                 | gaussdbformysql:proxy:delete                 | -              |
| GET /v3/{project_id}/instances/{instance_id}/proxies                  | gaussdbformysql:proxy:list                   | -              |
| GET /v3/{project_id}/instances/{instance_id}/proxy/flavors            | gaussdbformysql:proxy:listSpec               | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/enlarge           | gaussdbformysql:proxy:addNodes               | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/flavor  | gaussdbformysql:proxy:modifySpec             | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/weight  | gaussdbformysql:proxy:modifyWeight           | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/transaction-split | gaussdbformysql:proxy:modifyTransactionSplit | -              |
| POST /v3.1/{project_id}/instances/{instance_id}/error-logs            | gaussdbformysql:log:getErrorLogs             | -              |
| POST /v3.1/{project_id}/instances/{instance_id}/slow-logs             | gaussdbformysql:log:getSlowLogs              | -              |
| GET /v3/{project_id}/project-quotas                                   | gaussdbformysql:quota:list                   | -              |
| GET /v3/{project_id}/quotas                                           | gaussdbformysql:quota:list                   | -              |

| API                                                                           | Action                                                           | Dependen<br>cy |
|-------------------------------------------------------------------------------|------------------------------------------------------------------|----------------|
| POST /v3/{project_id}/quotas                                                  | gaussdbformysql:quota:mo<br>dify                                 | -              |
| PUT /v3/{project_id}/quotas                                                   | gaussdbformysql:quota:mo<br>dify                                 | -              |
| POST /v3/{project_id}/backups/<br>create                                      | gaussdbformysql:backup:cre<br>ate                                | -              |
| GET /v3/{project_id}/backups                                                  | gaussdbformysql:backup:list                                      | -              |
| GET /v3/{project_id}/instances/<br>{instance_id}/backups/policy               | gaussdbformysql:backup:list<br>Policy                            | -              |
| GET /v3/{project_id}/configurations                                           | gaussdbformysql:param:list                                       | -              |
| POST /v3/{project_id}/configurations                                          | gaussdbformysql:param:cre<br>ate                                 | -              |
| DELETE /v3/{project_id}/<br>configurations/{configuration_id}                 | gaussdbformysql:param:del<br>ete                                 | -              |
| GET /v3/{project_id}/configurations/<br>{configuration_id}                    | gaussdbformysql:param:get                                        | -              |
| PUT /v3/{project_id}/configurations/<br>{configuration_id}                    | gaussdbformysql:param:up<br>date                                 | -              |
| PUT /v3/{project_id}/configurations/<br>{configuration_id}/apply              | gaussdbformysql:param:app<br>ly                                  | -              |
| GET /v3/{project_id}/instances/<br>{instance_id}/tags                         | gaussdbformysql:tag:list                                         | -              |
| GET /v3/{project_id}/tags                                                     | gaussdbformysql:tag:list                                         | -              |
| POST /v3/{project_id}/instances/<br>{instance_id}/tags/action                 | gaussdbformysql:tag:deal                                         | -              |
| PUT /v3/{project_id}/instances/<br>{instance_id}/monitor-policy               | gaussdbformysql:instance:<br>modifySecondLevelMonitor-<br>Policy | -              |
| GET /v3/{project_id}/instances/<br>{instance_id}/monitor-policy               | gaussdbformysql:instance:g<br>etSecondLevelMonitoring-<br>Config | -              |
| POST /v3/{project_id}/instances/<br>{instance_id}/nodes/{node_id}/<br>restart | gaussdbformysql:instance:re<br>start                             | -              |
| POST /v3/{project_id}/instance/<br>{instance_id}/audit-log/switch             | gaussdbformysql:auditlog:o<br>perate                             | -              |

| API                                                                 | Action                                            | Dependen<br>cy |
|---------------------------------------------------------------------|---------------------------------------------------|----------------|
| GET /v3/{project_id}/instance/{instance_id}/audit-log/switch-status | gaussdbformysql:auditlog:li<br>st                 | -              |
| GET /v3/{project_id}/jobs                                           | gaussdbformysql:task:list                         | -              |
| POST /v3/{project_id}/instances/{instance_id}/db-users              | gaussdbformysql:user:creat<br>e                   | -              |
| GET /v3/{project_id}/instances/{instance_id}/db-users               | gaussdbformysql:user:list                         | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/db-users            | gaussdbformysql:user:delet<br>e                   | -              |
| PUT /v3/{project_id}/instances/{instance_id}/db-users/comment       | gaussdbformysql:user:modif<br>y                   | -              |
| PUT /v3/{project_id}/instances/{instance_id}/db-users/password      | gaussdbformysql:user:updat<br>ePassWord           | -              |
| POST /v3/{project_id}/instances/{instance_id}/db-users/privilege    | gaussdbformysql:user:grant<br>Privilege           | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/db-users/privilege  | gaussdbformysql:user:revok<br>ePrivilege          | -              |
| GET /v3/{project_id}/instances/{instance_id}/databases/charsets     | gaussdbformysql:database:l<br>ist                 | -              |
| POST /v3/{project_id}/instances/{instance_id}/databases             | gaussdbformysql:database:c<br>reate               | -              |
| GET /v3/{project_id}/instances/{instance_id}/databases              | gaussdbformysql:database:l<br>ist                 | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/databases           | gaussdbformysql:database:<br>delete               | -              |
| PUT /v3/{project_id}/instances/{instance_id}/databases/comment      | gaussdbformysql:database:<br>modify               | -              |
| POST /v3/{project_id}/instances/{instance_id}/sql-filter/switch     | gaussdbformysql:instance:s<br>etSqlFilterStatus   | -              |
| GET /v3/{project_id}/instances/{instance_id}/sql-filter/switch      | gaussdbformysql:instance:g<br>etSqlFilterStatus   | -              |
| PUT /v3/{project_id}/instances/{instance_id}/sql-filter/rules       | gaussdbformysql:instance:s<br>etSqlFilterRules    | -              |
| GET /v3/{project_id}/instances/{instance_id}/sql-filter/rules       | gaussdbformysql:instance:g<br>etSqlFilterRule     | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/sql-filter/rules    | gaussdbformysql:instance:d<br>eleteSqlFilterRules | -              |

| API                                                                               | Action                                           | Dependen<br>cy |
|-----------------------------------------------------------------------------------|--------------------------------------------------|----------------|
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/session-consistence | gaussdbformysql:proxy:modifyConsistency          | -              |
| GET /v3/{project_id}/immediate-jobs                                               | gaussdbformysql:task:list                        | -              |
| GET /v3/{project_id}/scheduled-jobs                                               | gaussdbformysql:task:list                        | -              |
| DELETE /v3/{project_id}/scheduled-jobs                                            | gaussdbformysql:task:delete                      | -              |
| DELETE /v3/{project_id}/jobs/{job_id}                                             | gaussdbformysql:task:delete                      | -              |
| POST /v3/{project_id}/instances/{instance_id}/db-upgrade                          | gaussdbformysql:instance:upgrade                 | -              |
| PUT /v3/{project_id}/instances/{instance_id}/ssl-option                           | gaussdbformysql:instance:modifySSL               | -              |
| PUT /v3/{project_id}/instances/{instance_id}/public-ips/bind                      | gaussdbformysql:instance:bindPublicIp            | -              |
| PUT /v3/{project_id}/instances/{instance_id}/public-ips/unbind                    | gaussdbformysql:instance:unbindPublicIp          | -              |
| PUT /v3/{project_id}/instances/{instance_id}/switchover                           | gaussdbformysql:instance:switchover              | -              |
| PUT /v3/{project_id}/instances/{instance_id}/ops-window                           | gaussdbformysql:instance:modifyMaintenanceWindow | -              |
| PUT /v3/{project_id}/instances/{instance_id}/security-group                       | gaussdbformysql:instance:modifySecurityGroup     | -              |
| PUT /v3/{project_id}/instances/{instance_id}/internal-ip                          | gaussdbformysql:instance:modifyVip               | -              |
| PUT /v3/{project_id}/instances/{instance_id}/port                                 | gaussdbformysql:instance:modifyPort              | -              |
| PUT /v3/{project_id}/instances/{instance_id}/alias                                | gaussdbformysql:instance:rename                  | -              |
| DELETE /v3/{project_id}/backups/{backup_id}                                       | gaussdbformysql:backup:delete                    | -              |
| POST /v3/{project_id}/instances/restore                                           | gaussdbformysql:instance:restoreInPlace          | -              |
| POST /v3/{project_id}/instances/{instance_id}/backups/encryption                  | gaussdbformysql:backup:encrypt                   | -              |

| API                                                                                | Action                                                | Dependen<br>cy |
|------------------------------------------------------------------------------------|-------------------------------------------------------|----------------|
| GET /v3/{project_id}/instances/{instance_id}/restore-time                          | gaussdbformysql:backup:getRestoreTime                 | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/connection-pool-type | gaussdbformysql:proxy:switchConnectionPoolType        | -              |
| POST /v3/{project_id}/instances/{instance_id}/dns                                  | gaussdbformysql:instance:createDns                    | -              |
| PUT /v3/{project_id}/instances/{instance_id}/dns                                   | gaussdbformysql:instance:modifyDns                    | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/port                 | gaussdbformysql:proxy:modifyPort                      | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/route-mode           | gaussdbformysql:proxy:modifyRouteMode                 | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/dns                  | gaussdbformysql:proxy:modifyDns                       | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/dns               | gaussdbformysql:proxy:deleteDns                       | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/ssl                  | gaussdbformysql:proxy:modifySSL                       | -              |
| PUT /v3/{project_id}/instances/{instance_id}/serverless/policy                     | gaussdbformysql:autoscaling:modifyPolicy              | -              |
| GET /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/processes             | gaussdbformysql:instance:listProcesses                | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/processes          | gaussdbformysql:instance:deleteProcesses              | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/reduce               | gaussdbformysql:proxy:deleteNodes                     | -              |
| GET /v3/{project_id}/instances/{instance_id}/serverless/policy                     | gaussdbformysql:serverless:getComputeAbilityPolicy    | -              |
| PUT /v3.1/{project_id}/instances/{instance_id}/serverless/policy                   | gaussdbformysql:serverless:updateComputeAbilityPolicy | -              |
| GET /v3/{project_id}/instances/{instance_id}/serverless/scaling-policy             | gaussdbformysql:serverless:getScalingPolicy           | -              |

| API                                                                     | Action                                            | Dependen<br>cy |
|-------------------------------------------------------------------------|---------------------------------------------------|----------------|
| PUT /v3/{project_id}/instances/{instance_id}/serverless/scaling-policy  | gaussdbformysql:serverless:updateScalingPolicy    | -              |
| POST /v3/{project_id}/instances/{instance_id}/backups/restore/tables    | gaussdbformysql:instance:tableRestore             | -              |
| GET /v3/{project_id}/instances/{instance_id}/backups/encryption         | gaussdbformysql:backup:encrypt                    | -              |
| GET /v3/{project_id}/instances/{instance_id}/incremental-backups        | gaussdbformysql:backup:list                       | -              |
| GET /v3.1/{project_id}/instances/{instance_id}/backups/restore/tables   | gaussdbformysql:backup:list                       | -              |
| -                                                                       | gaussdbformysql:backup:list                       | -              |
| PUT /v3/{project_id}/instances/{instance_id}/backups/offsite-policy     | gaussdbformysql:backup:modifyPolicy               | -              |
| POST /v3/{project_id}/instances/database-version/upgrade                | gaussdbformysql:instance:upgrade                  | -              |
| POST /v3/{project_id}/resource-check                                    | gaussdbformysql:instance:list                     | -              |
| GET /v3.1/{project_id}/instances/details                                | gaussdbformysql:instance:get                      | -              |
| GET /v3.1/{project_id}/instances                                        | gaussdbformysql:instance:list                     | -              |
| GET /v3/{project_id}/instances/recycle-info                             | gaussdbformysql:instance:list                     | -              |
| PUT /v3/{project_id}/instances/{instance_id}/storage/auto-expand-policy | gaussdbformysql:instance:modifyStorageSize        | -              |
| PUT /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/priority   | gaussdbformysql:instance:modifySwitchoverPriority | -              |
| PUT /v3/{project_id}/instances/{instance_id}/nodes/name                 | gaussdbformysql:instance:rename                   | -              |
| PUT /v3/{project_id}/instances/recycle-policy                           | gaussdbformysql:instance:setRecycleBin            | -              |
| GET /v3/{project_id}/instances/{instance_id}/storage/auto-expand-policy | gaussdbformysql:instance:get                      | -              |

| API                                                                       | Action                                   | Dependen<br>cy |
|---------------------------------------------------------------------------|------------------------------------------|----------------|
| GET /v3/{project_id}/instances/{instance_id}/auto-scaling/history         | gaussdbformysql:autoscaling:listHistory  | -              |
| GET /v3/{project_id}/instances/{instance_id}/auto-scaling/policy          | gaussdbformysql:autoscaling:listPolicy   | -              |
| GET /v3.1/{project_id}/instances/{instance_id}                            | gaussdbformysql:instance:get             | -              |
| GET /v3/{project_id}/instances/{instance_id}/eip                          | gaussdbformysql:instance:getPublicIp     | -              |
| GET /v3/{project_id}/instances/recycle-policy                             | gaussdbformysql:instance:setRecycleBin   | -              |
| GET /v3/{project_id}/instances/{instance_id}/table-info                   | gaussdbformysql:instance:get             | -              |
| PUT /v3/{project_id}/instances/{instance_id}/auto-scaling/policy          | gaussdbformysql:autoscaling:createPolicy | -              |
| GET /v3/{project_id}/instances/diagnosis-instance-count                   | gaussdbformysql:instance:list            | -              |
| GET /v3/{project_id}/instances/diagnosis-instance-infos                   | gaussdbformysql:instance:list            | -              |
| POST /v3/{project_id}/logs/lts-configs                                    | gaussdbformysql:log:createLtsConfig      | -              |
| DELETE /v3/{project_id}/logs/lts-configs                                  | gaussdbformysql:log:deleteLtsConfig      | -              |
| POST /v3/{project_id}/instances/{instance_id}/{node_id}/slowlog-download  | gaussdbformysql:log:getSlowLogs          | -              |
| GET /v3/{project_id}/instance/{instance_id}/auditlog/download-link        | gaussdbformysql:auditlog:list            | -              |
| GET /v3/{project_id}/instances/{instance_id}/audit-logs                   | gaussdbformysql:auditlog:list            | -              |
| PUT /v3/{project_id}/instances/{instance_id}/audit-log-policy             | gaussdbformysql:auditlog:operate         | -              |
| POST /v3/{project_id}/instances/{instance_id}/{node_id}/errorlog-download | gaussdbformysql:log:getErrorLogs         | -              |
| GET /v3/{project_id}/logs/lts-configs                                     | gaussdbformysql:log:listLtsConfig        | -              |
| GET /v3/{project_id}/instances/{instance_id}/slowlog/query                | gaussdbformysql:log:getSlowLogs          | -              |

| API                                                                                  | Action                                        | Dependen<br>cy |
|--------------------------------------------------------------------------------------|-----------------------------------------------|----------------|
| POST /v3/{project_id}/instances/{instance_id}/slow-logs/statistics                   | gaussdbformysql:log:getSlowLogs               | -              |
| POST /v3/{project_id}/instances/{instance_id}/slowlog/modify                         | gaussdbformysql:log:setSlowLogSensitiveStatus | -              |
| GET /v3/{project_id}/instances/{instance_id}/multi-tenant                            | gaussdbformysql:instance:get                  | -              |
| PUT /v3/{project_id}/instances/{instance_id}/multi-tenant                            | gaussdbformysql:instance:modify               | -              |
| POST /v3/{project_id}/configurations/{configuration_id}/copy                         | gaussdbformysql:param:create                  | -              |
| POST /v3/{project_id}/instances/{instance_id}/configurations/{configuration_id}/copy | gaussdbformysql:param:save                    | -              |
| POST /v3/{project_id}/configurations/comparison                                      | gaussdbformysql:param:get                     | -              |
| GET /v3/{project_id}/configurations/{configuration_id}/applicable-instances          | gaussdbformysql:param:list                    | -              |
| GET /v3/{project_id}/instances/{instance_id}/configurations                          | gaussdbformysql:param:getParameter            | -              |
| GET /v3/{project_id}/configurations/{configuration_id}/modify-history                | gaussdbformysql:param:list                    | -              |
| GET /v3/{project_id}/configurations/{config_id}/apply-history                        | gaussdbformysql:param:list                    | -              |
| PUT /v3/{project_id}/instances/{instance_id}/configurations                          | gaussdbformysql:param:update                  | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/access-control        | gaussdbformysql:proxy:modifyAccess            | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/dns                   | gaussdbformysql:proxy:createDns               | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/restart               | gaussdbformysql:proxy:restart                 | -              |
| GET /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/configurations         | gaussdbformysql:proxy:queryConfigurations     | -              |



| API                                                                                                 | Action                                          | Dependen<br>cy |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------|----------------|
| GET /v3/{project_id}/proxy/flavors                                                                  | gaussdbformysql:proxy:list                      | -              |
| GET /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/ipgroup                               | gaussdbformysql:proxy:modifyAccess              | -              |
| GET /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/{engine_name}/proxy-version           | gaussdbformysql:proxy:list                      | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/access-control-switch                | gaussdbformysql:proxy:modifyAccess              | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/new-node-auto-add                    | gaussdbformysql:proxy:create                    | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/rename                                | gaussdbformysql:proxy:rename                    | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/configurations                        | gaussdbformysql:proxy:updateConfigurations      | -              |
| POST /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/upgrade-version                      | gaussdbformysql:proxy:upgrade                   | -              |
| GET /v3/{project_id}/enterprise-projects                                                            | gaussdbformysql:instance:list                   | -              |
| DELETE /v3/{project_id}/instance/{instance_id}/scheduled-jobs                                       | gaussdbformysql:task:delete                     | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication/database-config-check | gaussdbformysql:htaplInstance:dbConfigCheck     | -              |
| POST /v3/{project_id}/configurations/starrocks/comparison                                           | gaussdbformysql:param:get                       | -              |
| POST /v3/{project_id}/starrocks/resource-check                                                      | gaussdbformysql:instance:list                   | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication/table-config-check    | gaussdbformysql:htaplInstance:tablesConfigCheck | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/users                                       | gaussdbformysql:htaplInstance:createUser        | -              |

| API                                                                                              | Action                                                | Dependen<br>cy |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------|----------------|
| POST /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication                    | gaussdbformysql:htapInsta<br>nce:createDataSync       | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks                                          | gaussdbformysql:htapInsta<br>nce:create               | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/starrocks/users                                  | gaussdbformysql:htapInsta<br>nce:deleteUser           | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication                  | gaussdbformysql:htapInsta<br>nce:deleteDataSync       | -              |
| DELETE /v3/{project_id}/instances/{instance_id}/starrocks/{starrocks_instance_id}                | gaussdbformysql:htapInsta<br>nce:delete               | -              |
| GET /v3/{project_id}/htap/datastores/{engine_name}                                               | gaussdbformysql:instance:li<br>stEngine               | -              |
| GET /v3/{project_id}/htap/flavors/{engine_name}                                                  | gaussdbformysql:instance:li<br>stSpec                 | -              |
| GET /v3/{project_id}/instances/{instance_id}/htap                                                | gaussdbformysql:htapInsta<br>nce:get                  | -              |
| GET /v3/{project_id}/htap/storage-type/{database}                                                | gaussdbformysql:htapInsta<br>nce:list                 | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/nodes                                     | gaussdbformysql:log:list                              | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/databases                                 | gaussdbformysql:htapInsta<br>nce:listDatabases        | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication/configuration       | gaussdbformysql:htapInsta<br>nce:getReplicationConfig | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication                     | gaussdbformysql:htapInsta<br>nce:getReplication       | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication/database-parameters | gaussdbformysql:htapInsta<br>nce:listDbParameter      | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/{starrocks_instance_id}                   | gaussdbformysql:htapInsta<br>nce:get                  | -              |

| API                                                                                          | Action                                       | Dependen<br>cy |
|----------------------------------------------------------------------------------------------|----------------------------------------------|----------------|
| PUT /v3/{project_id}/instances/{instance_id}/starrocks/security-group                        | gaussdbformysql:instance:modifySecurityGroup | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication/pause          | gaussdbformysql:htaplInstance:modifyDataSync | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/resize-flavor                        | gaussdbformysql:htaplInstance:modifySpec     | -              |
| PUT /v3/{project_id}/instances/{starrocks_instance_id}/starrocks/restart                     | gaussdbformysql:htaplInstance:restart        | -              |
| PUT /v3/{project_id}/instances/{starrocks_instance_id}/starrocks/{starrocks_node_id}/restart | gaussdbformysql:htaplInstance:restart        | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication/resume         | gaussdbformysql:htaplInstance:modifyDataSync | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/error-logs                           | gaussdbformysql:log:getErrorLogs             | -              |
| POST /v3/{project_id}/instances/{instance_id}/htap/databases                                 | gaussdbformysql:htaplInstance:listDatabases  | -              |
| POST /v3/{project_id}/instances/{instance_id}/htap/tables                                    | gaussdbformysql:htaplInstance:listDatabases  | -              |
| GET /v3/{project_id}/starrocks/instances/logs/lts-configs                                    | gaussdbformysql:log:listLtsConfig            | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/users                                 | gaussdbformysql:htaplInstance:listUser       | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/configurations                        | gaussdbformysql:param:getParameter           | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/users/sync                           | gaussdbformysql:htaplInstance:createUser     | -              |
| PUT /v3/{project_id}/instances/{instance_id}/starrocks/users/password                        | gaussdbformysql:htaplInstance:modifyPassword | -              |
| PUT /v3/{project_id}/instances/{instance_id}/starrocks/users/permission                      | gaussdbformysql:htaplInstance:grantUser      | -              |

| API                                                                                                   | Action                                            | Dependenc<br>y |
|-------------------------------------------------------------------------------------------------------|---------------------------------------------------|----------------|
| PUT /v3/{project_id}/instances/{instance_id}/starrocks/configurations                                 | gaussdbformysql:param:update                      | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/db-upgrade                                    | gaussdbformysql:instance:upgrade                  | -              |
| POST /v3/{project_id}/instances/{instance_id}/htap/template                                           | gaussdbformysql:htapInstance:listDatabases        | -              |
| GET /v3/{project_id}/instances/{instance_id}/database-version                                         | gaussdbformysql:instance:get                      | -              |
| PUT /v3/{project_id}/instances/{instance_id}/proxy/{proxy_id}/bind                                    | gaussdbformysql:proxy:bindEip                     | -              |
| GET /v3/{project_id}/instances/{instance_id}/audit-log-policy                                         | gaussdbformysql:auditlog:list                     | -              |
| POST /v3/{project_id}/instances/{instance_id}/audit-log-link                                          | gaussdbformysql:auditlog:list                     | -              |
| GET /v3/{project_id}/instances/{instance_id}/task-center-detail                                       | gaussdbformysql:task:list                         | -              |
| PUT /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication                          | gaussdbformysql:htapInstance:modifyDataSync       | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/databases/replication/configuration/{database} | gaussdbformysql:htapInstance:getReplicationConfig | -              |
| PUT /v3/{project_id}/instances/{instance_id}/query-queue/rules                                        | gaussdbformysql:param:update                      | -              |
| GET /v3/{project_id}/instances/{instance_id}/query-queue/rules                                        | gaussdbformysql:param:get                         | -              |
| POST /v3/{project_id}/instances/{instance_id}/htap/query-queue/switch                                 | gaussdbformysql:param:update                      | -              |
| POST /v3/{project_id}/instances/{instance_id}/starrocks/slow-logs                                     | gaussdbformysql:log:getSlowLogs                   | -              |
| GET /v3/{project_id}/instances/{instance_id}/starrocks/slowlog-sensitive                              | gaussdbformysql:log:getSlowLogs                   | -              |
| PUT /v3/{project_id}/instances/{instance_id}/starrocks/slowlog-sensitive                              | gaussdbformysql:log:setSlowLogSensitiveStatus     | -              |

## Resources

A resource type indicates the resources that a policy applies to. If you specify a resource type for any action in [Table 3-121](#), the resource URN must be specified in the policy statements using that action, and the policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the policy applies to all resources. You can also set condition keys in a policy to define resource types.

The following table lists the resource type that you can define in custom policies for TaurusDB.

**Table 3-121** Resource type supported by TaurusDB

| Resource Type | URN                                                          |
|---------------|--------------------------------------------------------------|
| instance      | gaussdbformysql:<region>:<account-id>:instance:<instance-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **gaussdbformysql:**) apply only to operations of the TaurusDB service. For details, see [Table 3-122](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can only be applied when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific Condition Keys Supported by TaurusDB

The following table lists the condition keys that you can define in identity policies for TaurusDB. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-122** Service-specific condition keys supported by TaurusDB

| Service-specific Condition Key                          | Type   | Single-valued/<br>Multivalued | Description                                                                                             |
|---------------------------------------------------------|--------|-------------------------------|---------------------------------------------------------------------------------------------------------|
| <a href="#">gaussdbformysql:FlavorType</a>              | String | Single-valued                 | Filters access by the specification type tag key that is passed in the request.                         |
| <a href="#">gaussdbformysql:SubnetId</a>                | String | Single-valued                 | Filters access by the subnet ID tag key that is passed in the request.                                  |
| <a href="#">gaussdbformysql:VpcId</a>                   | String | Single-valued                 | Filters access by the VPC ID tag key that is passed in the request.                                     |
| <a href="#">gaussdbformysql:ReplicationTargetRegion</a> | String | Single-valued                 | Filters access by the tag key that specifies the region a backup is to be replicated to in the request. |

### Examples of Condition Keys

- gaussdbformysql:FlavorType

For example, only Arm instances can be created.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "gaussdbformysql:instance:create"
      ],
      "Condition": {
        "StringEquals": {
          "gaussdbformysql:FlavorType": [
            "ARM"
          ]
        }
      }
    }
  ]
}
```

- gaussdbformysql:SubnetId

For example, only instances whose **SubnetId** is **SubnetId-a** can be created.

```
{
  "Version": "5.0",
  "Statement": [
```

```
{
  "Effect": "Allow",
  "Action": [
    "gaussdbformysql:instance:create"
  ],
  "Condition": {
    "StringEquals": {
      "gaussdbformysql:SubnetId": [
        "SubnetId-a"
      ]
    }
  }
}
```

- gaussdbformysql:VpcId

For example, only instances whose **VPC** is **vpcId-a** can be created.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "gaussdbformysql:instance:create"
      ],
      "Condition": {
        "StringEquals": {
          "gaussdbformysql:VpcId": [
            "vpcId-a"
          ]
        }
      }
    }
  ]
}
```

- gaussdbformysql:ReplicationTargetRegion

For example, cross-region backups can only be stored in the destination **region-a**.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "gaussdbformysql:backup:modifyPolicy"
      ],
      "Condition": {
        "StringEquals": {
          "gaussdbformysql:ReplicationTargetRegion": [
            "region-a"
          ]
        }
      }
    }
  ]
}
```

### 3.6.6 DAS

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the **Organizations** service also provides **Service Control Policy (SCP)** to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see **What Are the Differences in Access Control Between IAM and Organizations?**

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see **Creating a Custom Identity Policy**.
- For details about how to use these elements to create a custom SCP, see **Creating an SCP**.

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DAS, see **Resources**.

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DAS, see **Conditions**.

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see **Policies and Identity Policies**.



The following table lists the actions that you can define in identity policy statements for DAS.

**Table 3-123** Actions supported by DAS

| Action                                | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                               | Alias                  |
|---------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------|------------------------|
| das:instance:createConnection         | Grants the permission to add database connections.               | Write        | Instance                    | -                                                           | das:connections:create |
| das:connection:login                  | Grants the permission to connect to a DB instance.               | Write        | Connection                  | -                                                           | das:connections:login  |
| das:instance:dbLogin                  | Grants the permission to connect to a DB instance from DBS.      | Write        | Instance                    | -                                                           | das:connections:login  |
| das:connection:modify                 | Grants the permission to modify database connection information. | Write        | Connection                  | -                                                           | das:connections:modify |
| das:connection:delete                 | Grants the permission to delete database connection information. | Write        | Connection                  | -                                                           | das:connections:delete |
| das:connection:list                   | Grants the permission to obtain the connection information list. | List         | Connection                  | -                                                           | das:connections:list   |
| das:connection:createShareConnections | Grants the permission to create shared connections.              | Write        | Connection                  | das:TargetOrgPath<br>das:TargetOrgId<br>das:TargetAccountId | -                      |

| Action                                | Description                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| das:connection:cancelShareConnections | Grants the permission to delete shared connections.         | Write        | Connection                  | -             | -     |
| das:clouddba:getDbUser                | Grants the permission to obtain database user information.  | Read         | Instance                    | -             | -     |
| das:clouddba:registerDbUser           | Grants the permission to add database connections.          | Write        | Instance                    | -             | -     |
| das:clouddba:listDbUser               | Grants permission to query database users.                  | List         | Instance                    | -             | -     |
| das:clouddba:modifyDbUser             | Grants permission to change permissions of a database user. | Write        | Instance                    | -             | -     |
| das:clouddba:deleteDbUser             | Grants permission to delete a database user.                | Write        | Instance                    | -             | -     |
| das:clouddba:listInnoDBLock           | Grants the permission to display InnoDB lock waits.         | List         | Instance                    | -             | -     |
| das:clouddba:listMetadataLock         | Grants the permission to query metadata locks.              | List         | Instance                    | -             | -     |
| das:clouddba:deleteProcess            | Grants the permission to delete an instance session.        | Write        | Instance                    | -             | -     |

| Action                             | Description                                             | Access Level | Resource Type (*: required) | Condition Key | Alias                         |
|------------------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------|
| das:clouddba:listSlowSql           | Grants the permission to query the slow query logs.     | List         | Instance                    | -             | das:clouddba:slowSqlList      |
| das:clouddba:slowSqlExport         | Grants the permission to export slow query logs.        | List         | Instance                    | -             | -                             |
| das:clouddba:listFullSql           | Grants the permission to query the all query logs.      | List         | Instance                    | -             | das:clouddba:fullSqlList      |
| das:clouddba:fullSqlExport         | Grants the permission to export all query logs.         | List         | Instance                    | -             | -                             |
| das:clouddba:listTopSql            | Grants the permission to query the top SQL list.        | List         | Instance                    | -             | das:clouddba:topSqlList       |
| das:clouddba:listProcess           | Grants the permission to query sessions of an instance. | List         | Instance                    | -             | -                             |
| das:clouddba:changePaymentMode     | Grants the permission to set the payment mode.          | Write        | Instance                    | -             | -                             |
| das:clouddba:dailyReportsSubscribe | Grants the permission to subscribe to daily reports.    | Write        | Instance                    | -             | -                             |
| das:clouddba:listDailyReports      | Grants the permission to query daily reports.           | List         | Instance                    | -             | das:clouddba:dailyReportsList |

| Action                                | Description                                                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias                            |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------|
| das:clouddba:listSpaceAnalysis        | Grants the permission to query space diagnosis tasks.                                                           | List         | Instance                    | -             | -                                |
| das:clouddba:listSqlLimitRules        | Grants the permission to query SQL throttling rules.                                                            | List         | Instance                    | -             | -                                |
| das:clouddba:showSqlExecutionPlan     | Grants the permission to display SQL execution plans.                                                           | Read         | Connection Instance         | -             | das:clouddba:getSqlExecutionPlan |
| das:clouddba:sqlDiagnosis             | Grants the permission to perform SQL diagnosis.                                                                 | Write        | Connection Instance         | -             | -                                |
| das:clouddba:showSqlLimitJobInfo      | Grants permission to query SQL throttling task information.                                                     | Read         | Instance                    | -             | -                                |
| das:clouddba:showSqlLimitSwitchStatus | Grants the permission to query the SQL throttling status.                                                       | Read         | Instance                    | -             | -                                |
| das:clouddba:showSqlSwitchStatus      | Grants the permission to query the status of <b>Collect All Query Logs</b> and <b>Collect Slow Query Logs</b> . | Read         | Instance                    | -             | -                                |
| das:clouddba:deleteSqlLimitRules      | Grants the permission to delete SQL throttling rules.                                                           | Write        | Instance                    | -             | -                                |

| Action                                  | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias                          |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------|
| das:clouddba:modifySqlLimitRules        | Grants the permission to modify SQL throttling rules.                                                 | Write        | Instance                    | -             | -                              |
| das:clouddba:changeSqlLimitSwitchStatus | Grants the permission to modify the status of SQL throttling.                                         | Write        | Instance                    | -             | -                              |
| das:clouddba:changeSqlSwitch            | Grants the permission to configure <b>Collect All Query Logs</b> and <b>Collect Slow Query Logs</b> . | Write        | Instance                    | -             | -                              |
| das:clouddba:createSpaceAnalysisTask    | Grants the permission to create space diagnosis tasks.                                                | Write        | Instance                    | -             | -                              |
| das:clouddba:createSqlLimitRules        | Grants the permission to create SQL throttling rules.                                                 | Write        | Instance                    | -             | -                              |
| das:clouddba:executeSql                 | Grants the permission to execute SQL statements.                                                      | Write        | Instance                    | -             | -                              |
| das:clouddba:listBinlog                 | Grants the permission to view binlogs.                                                                | List         | Instance                    | -             | -                              |
| das:clouddba:createBinlogAnalysisTask   | Grants the permission to create a binlog parsing task.                                                | Write        | Instance                    | -             | -                              |
| das::addQuota                           | Grants the permission to add quotas.                                                                  | Write        | -                           | -             | das:clouddba:changePaymentMode |

| Action                             | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias                  |
|------------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------|
| das::showQuotas                    | Grants the permission to query resource quotas.                                        | Read         | -                           | -             | das:clouddba:menuList  |
| das::getSupported                  | Grants the permission to query the engine types supported in the current region.       | Read         | -                           | -             | das:connections:list   |
| das::getWhitelist                  | Grants the permission to query the function whitelist supported in the current region. | Read         | -                           | -             | das:connections:list   |
| das::listInstances                 | Grants the permission to query all types of DB instances.                              | List         | -                           | -             | das:connections:list   |
| das:instance:executeTestConnection | Grants the permission to execute a test connection.                                    | Write        | Instance                    | -             | das:connections:login  |
| das:connection:getSharedList       | Grants the permission to obtain the share list of a connection.                        | List         | Connection                  | -             | das:connections:list   |
| das:connection:updateSharedInfo    | Grants the permission to update a shared connection.                                   | Write        | Connection                  | -             | das:connections:modify |
| das:connection:getConnection       | Grants the permission to view connection information.                                  | Read         | Connection                  | -             | das:connections:list   |

| Action                            | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias                |
|-----------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------|
| das::getGlobalPrivacy             | Grants the permission to view the privacy statement.                        | Read         | -                           | -             | das:connections:list |
| das::putGlobalPrivacy             | Grants the permission to update the privacy description.                    | Write        | -                           | -             | das:connections:list |
| das::showCloudDBAInfo             | Grants the permission to view Intelligent O&M information.                  | Read         | -                           | -             | -                    |
| das:clouddba:showKillTaskSwitch   | Grants the permission to view the switch for continuously killing sessions. | Read         | Instance                    | -             | -                    |
| das:clouddba:changeKillTaskSwitch | Grants the permission to modify a task of continuously killing sessions.    | Write        | Instance                    | -             | -                    |
| das:clouddba:listKillTaskRecord   | Grants the permission to view tasks of continuously killing sessions.       | List         | Instance                    | -             | -                    |
| das:clouddba:createKillTask       | Grants the permission to create a task of continuously killing sessions.    | Write        | Instance                    | -             | -                    |
| das:clouddba:stopKillTask         | Grants the permission to stop a task of continuously killing sessions.      | Write        | Instance                    | -             | -                    |

| Action                               | Description                                  | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|----------------------------------------------|--------------|-----------------------------|---------------|-------|
| das:clouddba:buildInAccountLogin     | Logs in using a built-in account.            | Write        | Instance                    | -             | -     |
| das:clouddba:buildInAccountLogout    | Logs out a built-in account.                 | Write        | Instance                    | -             | -     |
| das:clouddba:changeTransactionSwitch | Enables or disables historical transactions. | Write        | Instance                    | -             | -     |
| das:clouddba:updateSqlLimitRules     | Modifies a SQL throttling rule.              | Write        | Instance                    | -             | -     |
| das::setMetricThreshold              | Sets metric thresholds.                      | Write        | -                           | -             | -     |

Each API of DAS usually supports one or more actions. [Table 3-124](#) lists the supported actions and dependencies.

**Table 3-124** Actions and dependencies supported by DAS APIs

| API                                                                   | Action                            | Dependencies |
|-----------------------------------------------------------------------|-----------------------------------|--------------|
| GET /v3/{project_id}/instances/{instance_id}/db-users                 | das:clouddba:listDbUser           | -            |
| POST /v3/{project_id}/instances/{instance_id}/db-users                | das:clouddba:registerDbUser       | -            |
| GET /v3/{project_id}/instances/{instance_id}/db-users/{db_user_id}    | das:clouddba:getDbUser            | -            |
| PUT /v3/{project_id}/instances/{instance_id}/db-users/{db_user_id}    | das:clouddba:modifyDbUser         | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/db-users/{db_user_id} | das:clouddba:deleteDbUser         | -            |
| GET /v3/{project_id}/instances/{instance_id}/sql/explain              | das:clouddba:showSqlExecutionPlan | -            |



| API                                                              | Action                                  | Dependencies |
|------------------------------------------------------------------|-----------------------------------------|--------------|
| POST /v3/{project_id}/instances/{instance_id}/sql/explain        | das:clouddba:showSqlExecutionPlan       | -            |
| GET /v3/{project_id}/instances/{instance_id}/processes           | das::showCloudDBAInfo                   | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/process          | das:clouddba:deleteProcess              | -            |
| GET /v3/{project_id}/instances/{instance_id}/metadata-locks      | das:clouddba:listMetadataLock           | -            |
| GET /v3/{project_id}/instances/{instance_id}/innodb-locks        | das:clouddba:listInnoDBLock             | -            |
| GET /v3/{project_id}/instances/{instance_id}/slow-query-logs     | das:clouddba:slowSqlExport              | -            |
| GET /v3/{project_id}/instances/{instance_id}/sql-statements      | das:clouddba:fullSqlExport              | -            |
| GET /v3/{project_id}/instances/{instance_id}/full-sql-tasks      | das:clouddba:listFullSql                | -            |
| GET /v3/{project_id}/instances/{instance_id}/full-sql-search     | das:clouddba:listFullSql                | -            |
| GET /v3/{project_id}/instances/{instance_id}/sql/switch          | das:clouddba:showSqlSwitchStatus        | -            |
| POST /v3/{project_id}/instances/{instance_id}/sql/switch         | das:clouddba:changeSqlSwitch            | -            |
| GET /v3/{project_id}/instances/{instance_id}/transaction/switch  | das::showCloudDBAInfo                   | -            |
| POST /v3/{project_id}/instances/{instance_id}/transaction/switch | das:clouddba:changeTransactionSwitch    | -            |
| GET /v3/{project_id}/instances/{instance_id}/transaction         | das::showCloudDBAInfo                   | -            |
| GET /v3/{project_id}/instances/{instance_id}/space-analysis      | das:clouddba:listSpaceAnalysis          | -            |
| POST /v3/{project_id}/instances/{instance_id}/space-analysis     | das:clouddba:createSpaceAnalysisTask    | -            |
| GET /v3/{project_id}/instances/{instance_id}/sql-limit/switch    | das:clouddba:showSqlLimitSwitchStatus   | -            |
| POST /v3/{project_id}/instances/{instance_id}/sql-limit/switch   | das:clouddba:changeSqlLimitSwitchStatus | -            |

| API                                                                                     | Action                           | Dependencies |
|-----------------------------------------------------------------------------------------|----------------------------------|--------------|
| GET /v3/{project_id}/instances/{instance_id}/sql-limit/job                              | das:clouddba:showSqlLimitJobInfo | -            |
| GET /v3/{project_id}/instances/{instance_id}/sql-limit/rules                            | das:clouddba:listSqlLimitRules   | -            |
| POST /v3/{project_id}/instances/{instance_id}/sql-limit/rules                           | das:clouddba:createSqlLimitRules | -            |
| DELETE /v3/{project_id}/instances/{instance_id}/sql-limit/rules                         | das:clouddba:deleteSqlLimitRules | -            |
| PUT /v3/{project_id}/instances/{instance_id}/sql-limit/rules                            | das:clouddba:updateSqlLimitRules | -            |
| POST /v3/{project_id}/instances/{instance_id}/sql-limit/parse                           | das:clouddba:createSqlLimitRules | -            |
| GET /v3/{project_id}/quotas                                                             | das::showQuotas                  | -            |
| GET /v3/{project_id}/instances/{instance_id}/top-sql-templates                          | das:clouddba:listTopSql          | -            |
| GET /v3/{project_id}/instances/{instance_id}/top-sql-trend                              | das:clouddba:listTopSql          | -            |
| GET /v3/{project_id}/instances/{instance_id}/slow-sql-templates                         | das:clouddba:slowSqlExport       | -            |
| GET /v3/{project_id}/instances/{instance_id}/slow-sql-trend                             | das:clouddba:slowSqlExport       | -            |
| POST /v3/{project_id}/instances/{instance_id}/slow-sql-statistics                       | das::showCloudDBAInfo            | -            |
| POST /v3/{project_id}/connections/{connection_id}/tuning/create-tuning                  | das:clouddba:sqlDiagnosis        | -            |
| GET /v3/{project_id}/connections/{connection_id}/tuning/{message_id}/show-tuning-result | das:clouddba:sqlDiagnosis        | -            |
| GET /v3/{project_id}/instances/top-risk                                                 | das::showCloudDBAInfo            | -            |
| GET /v3/{project_id}/instances/risk-trend                                               | das::showCloudDBAInfo            | -            |
| GET /v3/{project_id}/instances/distribution                                             | das::showCloudDBAInfo            | -            |
| GET /v3/{project_id}/instances/top-slow-log                                             | das::showCloudDBAInfo            | -            |

| API                                                                               | Action                                | Dependencies |
|-----------------------------------------------------------------------------------|---------------------------------------|--------------|
| GET /v3/{project_id}/instances/{instance_id}/top-slow-log                         | das::showCloudDBAInfo                 | -            |
| GET /v3/{project_id}/metric-names/support                                         | das::showCloudDBAInfo                 | -            |
| GET /v3/{project_id}/instance/nodes-info                                          | das::showCloudDBAInfo                 | -            |
| POST /v3/{project_id}/multi-nodes/single-metric                                   | das::showCloudDBAInfo                 | -            |
| GET /v3/{project_id}/get-risk-items                                               | das::showCloudDBAInfo                 | -            |
| POST /v3/{project_id}/set-metric-threshold                                        | das::setMetricThreshold               | -            |
| GET /v3/{project_id}/instances                                                    | das::listInstances                    | -            |
| POST /v3/{project_id}/instances/{instance_id}/create-instance-health-report-task  | das:clouddba:dailyReportsSubscribe    | -            |
| GET /v3/{project_id}/instances/{instance_id}/get-instance-health-report-task-list | das:clouddba:listDailyReports         | -            |
| GET /v3/{project_id}/instances/{instance_id}/get-instance-health-report           | das:clouddba:listDailyReports         | -            |
| POST /v3/{project_id}/instances/synchronize-instance-list                         | das::showCloudDBAInfo                 | -            |
| POST /v3/{project_id}/cloud-dba/change-payment-mode                               | das:clouddba:changePaymentMode        | -            |
| POST /v3/{project_id}/instances/{instance_id}/full-sql/add-task                   | das:clouddba:listFullSql              | -            |
| POST /v3/{project_id}/connections/share                                           | das:connection:createShareConnections | -            |
| DELETE /v3/{project_id}/connections/share                                         | das:connection:cancelShareConnections | -            |
| POST /v3/{project_id}/instances/{instance_id}/create-connection                   | das:instance:createConnection         | -            |
| GET /v3/{project_id}/list-connections                                             | das::showCloudDBAInfo                 | -            |
| POST /v3/{project_id}/instances/{instance_id}/login-built-in-account              | das:clouddba:builtinAccountlogin      | -            |

| API                                                                   | Action                            | Dependencies |
|-----------------------------------------------------------------------|-----------------------------------|--------------|
| POST /v3/{project_id}/instances/{instance_id}/logoff-built-in-account | das:clouddba:builtinAccountlogoff | -            |
| POST /v3/{project_id}/transaction/{instance_id}/create-export-task    | das::showCloudDBInfo              | -            |
| POST /v3/{project_id}/transaction/{instance_id}/delete-export-task    | das::showCloudDBInfo              | -            |
| GET /v3/{project_id}/transaction/{instance_id}/get-export-task-list   | das::showCloudDBInfo              | -            |
| GET /v3/{project_id}/transaction/{instance_id}/get-export-task-info   | das::showCloudDBInfo              | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-125](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DAS.

**Table 3-125** Resource types supported by DAS

| Resource Type | URN                                                  | Condition Key |
|---------------|------------------------------------------------------|---------------|
| Instance      | das:<region>:<account-id>:instance:<instance-id>     | -             |
| Connection    | das:<region>:<account-id>:connection:<connection-id> | -             |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- A key in the **Condition** element of a statement can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the

system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).

- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **DAS:**) apply only to operations of DAS. For details, see [Table 3-126](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can only be applied when its request conditions are met. For supported condition operators, see [condition operators](#).

The following table lists the condition keys that you can define in custom policies for DAS. You can use these condition keys to specify additional conditions under which the policy is applied.

**Table 3-126** Service-specific condition keys supported by DAS

| Service-specific Condition Key   | Type   | Description                                                                       |
|----------------------------------|--------|-----------------------------------------------------------------------------------|
| <code>das:TargetOrgPath</code>   | String | Controls permissions of target shared accounts based on their organization paths. |
| <code>das:TargetOrgId</code>     | String | Controls permissions of target shared accounts based on their organization IDs.   |
| <code>das:TargetAccountId</code> | String | Controls permissions of target shared accounts based on their IDs.                |

## 3.7 Security & Compliance

### 3.7.1 Data Encryption Workshop (DEW)

#### 3.7.1.1 Key Management Service (KMS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by KMS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by KMS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for KMS.

**Table 3-127** Actions supported by KMS

| Action         | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|----------------|-----------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:cmk:create | Grants permission to create KMS keys.                           | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> </ul>                                                                                                             | -     |
|                |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• g:EnterpriseProjectId</li> <li>• g:RequestTag/&lt;tag-key&gt;</li> <li>• g:TagKeys</li> </ul>                                                                                       |       |
| kms:cmk:list   | Grants permission to View All KMS Key Information.              | List         | KeyId*                      | -                                                                                                                                                                                                                            | -     |
|                |                                                                 |              | -                           | g:EnterpriseProjectId                                                                                                                                                                                                        |       |
| kms:cmk:enable | Grants permission to change the status of a KMS key to Enabled. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action          | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|-----------------|---------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:cmk:disable | Grants permission to disable KMS keys.            | Write        | KeyId<br>*                  | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| kms:cmk:get     | Grants permission to view details about KMS keys. | Read         | KeyId<br>*                  | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                 |                                                   |              | -                           | <ul style="list-style-type: none"> <li>• kms:RequestAlias</li> <li>• kms:ResourceAliases</li> </ul>                                                                                                                          |       |



| Action                             | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias                                                              |
|------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| kms:cmk:createDataKey              | Grants permission to use KMS keys to generate data keys.                                        | Write        | KeyId<br>*                  | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:dek:create</li> </ul> |
|                                    |                                                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:RecipientAttestation</a></li> <li>• <a href="#">kms:RequestAlias</a></li> <li>• <a href="#">kms:ResourceAliases</a></li> <li>• <a href="#">kms:EncryptionContext</a></li> </ul>                                                                                     |                                                                    |
| kms:cmk:createDataKeyWithPlaintext | Grants permission to use KMS keys to generate data keys that do not contain plaintext versions. | Write        | KeyId<br>*                  | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:dek:create</li> </ul> |

| Action                 | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias                                                                                         |
|------------------------|--------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|                        |                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:RequestAlias</a></li> <li>• <a href="#">kms:ResourceAliases</a></li> <li>• <a href="#">kms:EncryptionContext</a></li> </ul>                                                                                                                                         |                                                                                               |
| kms:cmk:encryptDataKey | Grants permission to encrypt the data key. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:dek:crypto</li> <li>• kms:dek:encrypt</li> </ul> |
|                        |                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:RequestAlias</a></li> <li>• <a href="#">kms:ResourceAliases</a></li> <li>• <a href="#">kms:EncryptionContext</a></li> </ul>                                                                                                                                         |                                                                                               |

| Action                 | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias                                                                                         |
|------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| kms:cmk:decryptDataKey | Grants permission to decrypt the data key.                            | Write        | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>• kms:dek:crypto</li> <li>• kms:dek:decrypt</li> </ul> |
|                        |                                                                       |              | -                           | <ul style="list-style-type: none"> <li>• kms:RecipientAttestation</li> <li>• kms:RequestAlias</li> <li>• kms:ResourceAliases</li> <li>• kms:EncryptionContext</li> </ul>                                                     |                                                                                               |
| kms:cmk:encryptData    | Grants permission to use the specified KMS key to encrypt small data. | Write        | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>• kms:cmk:crypto</li> <li>• kms:cmk:encrypt</li> </ul> |

| Action              | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias                                                                                         |
|---------------------|----------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|                     |                                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:EncryptionAlgorithm</a></li> <li>• <a href="#">kms:RequestAlias</a></li> <li>• <a href="#">kms:ResourceAliases</a></li> <li>• <a href="#">kms:EncryptionContext</a></li> </ul>                                                                                      |                                                                                               |
| kms:cmk:decryptData | Grants permission to decrypt data using the specified KMS key. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:cmk:crypto</li> <li>• kms:cmk:decrypt</li> </ul> |
|                     |                                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:EncryptionAlgorithm</a></li> <li>• <a href="#">kms:RecipientAttestation</a></li> <li>• <a href="#">kms:RequestAlias</a></li> <li>• <a href="#">kms:ResourceAliases</a></li> <li>• <a href="#">kms:EncryptionContext</a></li> </ul>                                  |                                                                                               |

| Action              | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                    | Alias                                                              |
|---------------------|-------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| kms::generateRandom | Grants permission to generate secure random strings.  | Write        | -                           | <a href="#">kms:RecipientAttestation</a>                                                                                                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>kms:cmk:generate</li> </ul> |
| kms:cmk:sign        | Grants permission to generate digital signatures for. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li><a href="#">kms:KeyOrigin</a></li> <li><a href="#">kms:KeySpec</a></li> <li><a href="#">kms:KeyUsage</a></li> <li><a href="#">kms:MultiRegionKeyType</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                                                                  |
|                     |                                                       |              | -                           | <ul style="list-style-type: none"> <li><a href="#">kms:MessageType</a></li> <li><a href="#">kms:SigningAlgorithm</a></li> <li><a href="#">kms:RequestAlias</a></li> <li><a href="#">kms:ResourceAliases</a></li> </ul>                                                                                           |                                                                    |

| Action              | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|---------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:cmk:verify      | Grants permission to use the specified KMS key to verify the digital signature. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                     |                                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• kms:MessageType</li> <li>• kms:SigningAlgorithm</li> <li>• kms:RequestAlias</li> <li>• kms:ResourceAliases</li> </ul>                                                               |       |
| kms:cmk:generateMac | Grants permission to generate a MAC.                                            | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action            | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias |
|-------------------|--------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                   |                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:MacAlgorithm</a></li> <li>• <a href="#">kms:RequestAlias</a></li> <li>• <a href="#">kms:ResourceAliases</a></li> </ul>                                                                                                                                              |       |
| kms:cmk:verifyMac | Grants permission to verify a MAC using a specified KMS key. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
|                   |                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:MacAlgorithm</a></li> <li>• <a href="#">kms:RequestAlias</a></li> <li>• <a href="#">kms:ResourceAliases</a></li> </ul>                                                                                                                                              |       |

| Action               | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias                                                                   |
|----------------------|---------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| kms:cmk:getPublicKey | Grants permission to query the KMS key and public key.              | Read         | KeyId<br>*                  | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                                                       |
|                      |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• kms:RequestAlias</li> <li>• kms:ResourceAliases</li> </ul>                                                                                                                          |                                                                         |
| kms::getVersions     | Grants permission to query service versions.                        | Read         | -                           | -                                                                                                                                                                                                                            | -                                                                       |
| kms::getVersion      | Grants permission to query the service key API version.             | Read         | -                           | -                                                                                                                                                                                                                            | -                                                                       |
| kms::getInstance     | Grants permission to query the number of key instances to the user. | Read         | -                           | -                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• kms:cmk:getInstance</li> </ul> |
| kms::getQuota        | Grants permission to query user quotas.                             | Read         | -                           | -                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• kms:cmk:getQuota</li> </ul>    |



| Action                      | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias                                                              |
|-----------------------------|-----------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| kms:cmk:scheduleKeyDeletion | Grants permission to periodically delete KMS keys.              | Write        | KeyId<br>*                  | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:cmk:update</li> </ul> |
|                             |                                                                 |              | -                           | <a href="#">kms:ScheduleKeyDeletionPendingWindowInDays</a>                                                                                                                                                                                                                                                                   |                                                                    |
| kms:cmk:cancelKeyDeletion   | Grants permission to cancel the scheduled deletion of KMS keys. | Write        | KeyId<br>*                  | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:cmk:update</li> </ul> |

| Action                       | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias                                                              |
|------------------------------|--------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| kms:cmk:updateKeyAlias       | Grants permission to change key aliases.         | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:cmk:update</li> </ul> |
| kms:cmk:updateKeyDescription | Grants permission to change the key description. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:cmk:update</li> </ul> |

| Action              | Description                                                 | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias              |
|---------------------|-------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| kms:cmk:createGrant | Grants permission to a specific key creation authorization. | Permission_management | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • kms:grant:create |
|                     |                                                             |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">kms:GranteePrincipalType</a></li> <li>• <a href="#">kms:GrantOperations</a></li> <li>• <a href="#">kms:GranteePrincipal</a></li> <li>• <a href="#">kms:RetiringPrincipal</a></li> </ul>                                                                                 |                    |

| Action                   | Description                                                                         | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias                                                                |
|--------------------------|-------------------------------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| kms:cmk:listGrants       | Grants permission to query the list of granted permissions for a specific key.      | List                  | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>• kms:grant:list</li> </ul>   |
| kms::listRetirableGrants | Grants permission to query the list of authorizations that can be retired for keys. | List                  | -                           | -                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• kms:grant:list</li> </ul>   |
| kms:cmk:retireGrant      | Grants permission to a specific key retiring authorization.                         | Permission_management | KeyId*                      | g:ResourceTag/<tag-key>                                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• kms:grant:retire</li> </ul> |

| Action              | Description                                                   | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias              |
|---------------------|---------------------------------------------------------------|-----------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| kms:cmk:revokeGrant | Grants permission to revoke authorization for a specific key. | Permission_management | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | • kms:grant:revoke |
| kms:cmk:getMaterial | Grants permission to obtain key import parameters.            | Read                  | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                  |
|                     |                                                               |                       | -                           | kms:WrappingAlgorithm                                                                                                                                                                                                        |                    |

| Action                 | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|------------------------|--------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:cmk:importMaterial | Grants permission to import key materials. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                        |                                            |              | -                           | kms:ExpirationTime                                                                                                                                                                                                           |       |
| kms:cmk:deleteMaterial | Grants permission to delete key materials. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                 | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|------------------------|----------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:cmk:enableRotation | Grants permission to enable rotation of a specified key.       | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| kms:cmk:updateRotation | Grants permission to change the specified key rotation period. | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                  | Description                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|-------------------------|--------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:cmk:disableRotation | Grants permission to disable key rotation.                         | Write        | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| kms:cmk:getRotation     | Grants permission to query the rotation status of a specified key. | Read         | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| kms:keystore:create     | Grants permission to create a dedicated keystore.                  | Write        | keystore *                  | -                                                                                                                                                                                                                            | -     |
| kms:keystore:delete     | Grants permission to delete the dedicated keystore.                | Write        | keystore *                  | -                                                                                                                                                                                                                            | -     |



| Action               | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias               |
|----------------------|------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| kms:keystore:enable  | Grants permission to enable the dedicated keystore.        | Write        | keystore *                  | -                                                                                                                                                                                                                                                                                                                            | -                   |
| kms:keystore:disable | Grants permission to disable the dedicated keystore.       | Write        | keystore *                  | -                                                                                                                                                                                                                                                                                                                            | -                   |
| kms:keystore:list    | Grants permission to query the list of dedicated keystore. | List         | keystore *                  | -                                                                                                                                                                                                                                                                                                                            | -                   |
| kms:keystore:get     | Grants permission to obtain the dedicated keystore.        | Read         | keystore *                  | -                                                                                                                                                                                                                                                                                                                            | -                   |
| kms:cmk:createTag    | Grants permission to add tags to a specified CMK.          | Tagging      | KeyId *                     | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • kms:cmkTag:create |
|                      |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                                                                        |                     |

| Action                | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias                     |
|-----------------------|-------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| kms:cmk:createTags    | Grants permission to add or delete tags in batches for a specified CMK. | Tagging      | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • kms:cmkTag:batch        |
|                       |                                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                                                                                                        |                           |
| kms:cmk:listKeysByTag | Grants permission to query a specified key instance.                    | List         | KeyId*                      | -                                                                                                                                                                                                                                                                                                                            | • kms:cmkTag:listInstance |
| kms:cmk:deleteTag     | Grants permission to delete a specified key tag.                        | Tagging      | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • kms:cmkTag:delete       |

| Action            | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                | Alias                                                               |
|-------------------|------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
|                   |                                                                  |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                                                                                    |                                                                     |
| kms:cmk:getTags   | Grants permission to query a specified key tag.                  | Read         | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• kms:cmkTag:list</li> </ul> |
| kms::listAllTags  | Grants permission to query the label of a specified key project. | List         | -                           | -                                                                                                                                                                                                                                                                                                                            | -                                                                   |
| kms:cmk:replicate | Grants permission to replicate KMS keys.                         | Write        | KeyId*                      | <ul style="list-style-type: none"> <li>• <a href="#">kms:KeyOrigin</a></li> <li>• <a href="#">kms:KeySpec</a></li> <li>• <a href="#">kms:KeyUsage</a></li> <li>• <a href="#">kms:MultiRegionKeyType</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                                                                   |

| Action                      | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|-----------------------------|---------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:cmk:updatePrimaryRegion | Grants permission to update primary region of KMS keys. | Write        | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                             |                                                         |              | -                           | kms:PrimaryRegion                                                                                                                                                                                                            |       |
| kms:alias:create            | Grants permission to update primary region of KMS keys. | Write        | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                             |                                                         |              | alias *                     | -                                                                                                                                                                                                                            |       |

| Action              | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                | Alias |
|---------------------|---------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| kms:alias:delete    | Grants permission to update primary region of KMS keys. | Write        | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                     |                                                         |              | alias *                     | -                                                                                                                                                                                                                            |       |
| kms:alias:list      | Grants permission to update primary region of KMS keys. | List         | -                           | -                                                                                                                                                                                                                            | -     |
| kms:alias:associate | Grants permission to update primary region of KMS keys. | Write        | KeyId *                     | <ul style="list-style-type: none"> <li>• kms:KeyOrigin</li> <li>• kms:KeySpec</li> <li>• kms:KeyUsage</li> <li>• kms:MultiRegionKeyType</li> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                     |                                                         |              | alias *                     | -                                                                                                                                                                                                                            |       |

Each API of KMS usually supports one or more actions. [Table 3-128](#) lists the supported actions and dependencies.

**Table 3-128** Actions and dependencies supported by KMS APIs

| API                                                          | Action                                | Dependencies |
|--------------------------------------------------------------|---------------------------------------|--------------|
| POST /v1.0/{project_id}/kms/create-key                       | kms:cmk:create                        | -            |
| POST /v1.0/{project_id}/kms/list-keys                        | kms:cmk:list                          | -            |
| POST /v1.0/{project_id}/kms/enable-key                       | kms:cmk:enable                        | -            |
| POST /v1.0/{project_id}/kms/disable-key                      | kms:cmk:disable                       | -            |
| POST /v1.0/{project_id}/kms/describe-key                     | kms:cmk:get                           | -            |
| POST /v1.0/{project_id}/kms/create-datakey                   | kms:cmk:createDataKey                 | -            |
| POST /v1.0/{project_id}/kms/create-datakey-without-plaintext | kms:cmk:createDataKeyWithoutPlaintext | -            |
| POST /v1.0/{project_id}/kms/encrypt-datakey                  | kms:cmk:encryptDataKey                | -            |
| POST /v1.0/{project_id}/kms/decrypt-datakey                  | kms:cmk:decryptDataKey                | -            |
| POST /v1.0/{project_id}/kms/encrypt-data                     | kms:cmk:encryptData                   | -            |
| POST /v1.0/{project_id}/kms/decrypt-data                     | kms:cmk:decryptData                   | -            |
| POST /v1.0/{project_id}/kms/gen-random                       | kms::generateRandom                   | -            |

| API                                                | Action                       | Dependencies |
|----------------------------------------------------|------------------------------|--------------|
| POST /v1.0/{project_id}/kms/sign                   | kms:cmk:sign                 | -            |
| POST /v1.0/{project_id}/kms/verify                 | kms:cmk:verify               | -            |
| POST /v1.0/{project_id}/kms/generate-mac           | kms:cmk:generateMac          | -            |
| POST /v1.0/{project_id}/kms/verify-mac             | kms:cmk:verifyMac            | -            |
| POST /v1.0/{project_id}/kms/get-publickey          | kms:cmk:getPublicKey         | -            |
| GET /                                              | kms::getVersions             | -            |
| GET /{version_id}                                  | kms::getVersion              | -            |
| POST /v1.0/{project_id}/kms/schedule-key-deletion  | kms:cmk:scheduleKeyDeletion  | -            |
| POST /v1.0/{project_id}/kms/cancel-key-deletion    | kms:cmk:cancelKeyDeletion    | -            |
| GET /v1.0/{project_id}/kms/user-instances          | kms::getInstance             | -            |
| GET /v1.0/{project_id}/kms/user-quotas             | kms::getQuota                | -            |
| POST /v1.0/{project_id}/kms/update-key-alias       | kms:cmk:updateKeyAlias       | -            |
| POST /v1.0/{project_id}/kms/update-key-description | kms:cmk:updateKeyDescription | -            |
| POST /v1.0/{project_id}/kms/create-grant           | kms:cmk:createGrant          | -            |

| API                                                      | Action                   | Dependencies |
|----------------------------------------------------------|--------------------------|--------------|
| POST /v1.0/{project_id}/kms/list-grants                  | kms:cmk:listGrants       | -            |
| POST /v1.0/{project_id}/kms/list-retirable-grants        | kms::listRetirableGrants | -            |
| POST /v1.0/{project_id}/kms/retire-grant                 | kms:cmk:retireGrant      | -            |
| POST /v1.0/{project_id}/kms/revoke-grant                 | kms:cmk:revokeGrant      | -            |
| POST /v1.0/{project_id}/kms/get-parameters-for-import    | kms:cmk:getMaterial      | -            |
| POST /v1.0/{project_id}/kms/import-key-material          | kms:cmk:importMaterial   | -            |
| POST /v1.0/{project_id}/kms/delete-imported-key-material | kms:cmk:deleteMaterial   | -            |
| POST /v1.0/{project_id}/kms/enable-key-rotation          | kms:cmk:enableRotation   | -            |
| POST /v1.0/{project_id}/kms/update-key-rotation-interval | kms:cmk:updateRotation   | -            |
| POST /v1.0/{project_id}/kms/disable-key-rotation         | kms:cmk:disableRotation  | -            |
| POST /v1.0/{project_id}/kms/get-key-rotation-status      | kms:cmk:getRotation      | -            |
| POST /v1.0/{project_id}/keystores                        | kms:keystore:create      | -            |



| API                                                     | Action                | Dependencies |
|---------------------------------------------------------|-----------------------|--------------|
| DELETE /v1.0/{project_id}/keystores/{keystore_id}       | kms:keystore:delete   | -            |
| POST /v1.0/{project_id}/keystores/{keystore_id}/enable  | kms:keystore:enable   | -            |
| POST /v1.0/{project_id}/keystores/{keystore_id}/disable | kms:keystore:disable  | -            |
| GET /v1.0/{project_id}/keystores                        | kms:keystore:list     | -            |
| GET /v1.0/{project_id}/keystores/{keystore_id}          | kms:keystore:get      | -            |
| POST /v1.0/{project_id}/kms/{key_id}/tags               | kms:cmk:createTag     | -            |
| POST /v1.0/{project_id}/kms/{key_id}/tags/action        | kms:cmk:createTags    | -            |
| POST /v1.0/{project_id}/kms/{resource_instances}/action | kms:cmk:listKeysByTag | -            |
| DELETE /v1.0/{project_id}/kms/{key_id}/tags/{key}       | kms:cmk:deleteTag     | -            |
| GET /v1.0/{project_id}/kms/{key_id}/tags                | kms:cmk:getTags       | -            |
| GET /v1.0/{project_id}/kms/tags                         | kms::listAllTags      | -            |

| API                                                          | Action                      | Dependencies |
|--------------------------------------------------------------|-----------------------------|--------------|
| POST /v2/{project_id}/kms/keys/{key_id}/replicate            | kms:cmk:replicate           | -            |
| PUT /v2/{project_id}/kms/keys/{key_id}/update-primary-region | kms:cmk:updatePrimaryRegion | -            |
| POST /v1.0/{project_id}/kms/aliases                          | kms:alias:create            | -            |
| DELETE /v1.0/{project_id}/kms/aliases                        | kms:alias:delete            | -            |
| GET /v1.0/{project_id}/kms/aliases                           | kms:alias:list              | -            |
| POST /v1.0/{project_id}/kms/alias/associate                  | kms:alias:associate         | -            |
| POST /v1.0/{project_id}/kms/create-pin                       | kms:cmk:createDataKey       | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-129](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for KMS.

**Table 3-129** Resource types supported by KMS

| Resource Type | URN                                          |
|---------------|----------------------------------------------|
| KeyId         | kms:<region>:<account-id>:KeyId:<cmk-id>     |
| alias         | kms:<region>:<account-id>:alias:<alias-name> |

| Resource Type | URN                                              |
|---------------|--------------------------------------------------|
| keystore      | kms:<region>:<account-id>:keystore:<keystore-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, kms) apply only to operations of the xx service. For details, see [Table 3-130](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by KMS

The following table lists the condition keys that you can define in identity policies for KMS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-130** Service-specific condition keys supported by KMS

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                                           |
|--------------------------------|--------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| kms:EncryptionAlgorithm        | string | Single-valued                 | Filters access to encryption/decryption operations based on the encryption/decryption algorithm value in the request. |
| kms:GranteePrincipal-Type      | string | Single-valued                 | Filters access to the CreateGrant operation based on the authorization principal type constraint in the request.      |
| kms:GrantOperations            | string | Multivalued                   | Filters access to the CreateGrant operation based on the operation to be authorized.                                  |
| kms:GranteePrincipal           | string | Single-valued                 | Filters access to the CreateGrant operation based on the authorized party principal in the authorization.             |
| kms:KeyOrigin                  | string | Single-valued                 | Filters access to an API operation based on the origin attribute of the KMS key created or used for the operation.    |
| kms:KeySpec                    | string | Single-valued                 | Filters access to API operations based on the key_spec attribute that created or used the operation KMS key.          |
| kms:KeyUsage                   | string | Single-valued                 | Filters access to API operations based on the key_usage attribute of the KMS key created or used for the operation.   |

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                                                                                                                        |
|--------------------------------|--------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| kms:MessageType                | string | Single-valued                 | Filters access to signing and verifying signature operations based on the value of the message_type parameter in the request.                                                                      |
| kms:RetiringPrincipal          | string | Single-valued                 | Filters access to CreateGrant operations based on retiring_principal in authorization.                                                                                                             |
| kms:SigningAlgorithm           | string | Single-valued                 | Filters access to signing and verifying operations based on signing_algorithm in the request.                                                                                                      |
| kms:ExpirationTime             | date   | Single-valued                 | Filters access to the ImportKeyMaterial operation based on the value of the expiration_time parameter in the request.                                                                              |
| kms:WrappingAlgorithm          | string | Single-valued                 | Filters access to the CreateParametersForImport operation based on the value of the wrapping_algorithm parameter in the request.                                                                   |
| kms:RecipientAttestation       | string | Single-valued                 | Filters access to the CreateDatakey, DecryptData, DecryptDatakey, and CreateRandom operations based on the Platform Configuration Register (PCR) value of the attestation document in the request. |

| Service-specific Condition Key             | Type    | Single-valued/<br>Multivalued | Description                                                                                         |
|--------------------------------------------|---------|-------------------------------|-----------------------------------------------------------------------------------------------------|
| kms:MacAlgorithm                           | string  | Single-valued                 | Filters access to MAC generation and verification operations based on mac_algorithm in the request. |
| kms:RequestAlias                           | string  | Single-valued                 | Filters access to MAC generation and verification operations based on mac_algorithm in the request. |
| kms:ResourceAliases                        | string  | Multivalued                   | Filters access to MAC generation and verification operations based on mac_algorithm in the request. |
| kms:MultiRegionKeyType                     | string  | Single-valued                 | Filters access to API operations based on MultiRegionKeyType in the KMS key field.                  |
| kms:PrimaryRegion                          | string  | Single-valued                 | Filters access to API operations based on primary_region in the request.                            |
| kms:EncryptionContext                      | string  | Single-valued                 | Filters access to API operations based on additional_authenticated_data in the request.             |
| kms:ScheduleKeyDeletionPendingWindowInDays | numeric | Single-valued                 | Filters access to API operations based on pending_days in the request.                              |

### 3.7.1.2 Key Pair Service (KPS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by KPS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by KPS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for KPS.

**Table 3-131** Actions supported by KPS

| Action                | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                             | Alias                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| kps:SSHKeyPair:create | Grants permission to create and import an SSH key pair.         | Write        | SSHKeyPair*                 | <ul style="list-style-type: none"> <li>• <a href="#">kps:KmsKeyId</a></li> <li>• <a href="#">kps:Algorithm</a></li> </ul> | <ul style="list-style-type: none"> <li>• kps:domainKeypairs:create</li> </ul>                                                           |
| kps:SSHKeyPair:delete | Grants permission to delete an SSH key pair.                    | Write        | SSHKeyPair*                 | -                                                                                                                         | <ul style="list-style-type: none"> <li>• kps:domainKeypairs:delete</li> </ul>                                                           |
| kps:SSHKeyPair:get    | Grants permission to query the details about an SSH key pair.   | Read         | SSHKeyPair*                 | -                                                                                                                         | <ul style="list-style-type: none"> <li>• kps:domainKeypairs:get</li> </ul>                                                              |
| kps:SSHKeyPair:list   | Grants permission to query the SSH key pairs list.              | List         | SSHKeyPair*                 | -                                                                                                                         | <ul style="list-style-type: none"> <li>• kps:domainKeypairs:list</li> </ul>                                                             |
| kps:SSHKeyPair:update | Grants permission to update the description of an SSH key pair. | Write        | SSHKeyPair*                 | -                                                                                                                         | <ul style="list-style-type: none"> <li>• kps:domainKeypairs:update</li> </ul>                                                           |
| kps:SSHKeyPair:bind   | Grants permission to bind ECS to a new SSH key pair.            | Write        | SSHKeyPair*                 | -                                                                                                                         | <ul style="list-style-type: none"> <li>• kps:domainKeypairs:bind</li> </ul>                                                             |
| kps::deleteFailedTask | Grants permission to delete failed tasks.                       | Write        | -                           | -                                                                                                                         | <ul style="list-style-type: none"> <li>• kps:domainKeypairs:deletefailedtask</li> <li>• kps:domainKeypairs:deletefailedtasks</li> </ul> |



| Action                           | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                          |
|----------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------------------------------------------|
| kps::SSHKeyPair:unbind           | Grants permission to unbind ECS from an SSH key pair.         | Write        | SSHKeyPair *                | -             | <ul style="list-style-type: none"> <li>kps:domainKeypairs:unbind</li> <li>ecs:serverKeypairs:unbind</li> </ul> |
| kps::getFailedTask               | Grants permission to query information about failed tasks.    | List         | -                           | -             | <ul style="list-style-type: none"> <li>kps:domainKeypairs:getfailtask</li> </ul>                               |
| kps::getTask                     | Grants permission to query the current task execution status. | List         | -                           | -             | <ul style="list-style-type: none"> <li>kps:domainKeypairs:gettask</li> </ul>                                   |
| kps::getRunningTask              | Grants permission to query information about ongoing tasks.   | List         | -                           | -             | <ul style="list-style-type: none"> <li>kps:domainKeypairs:getrunningtask</li> </ul>                            |
| kps::SSHKeyPair:importPrivateKey | Grants permission to import a private key to a key pair.      | Write        | SSHKeyPair *                | kps::KmsKeyId | <ul style="list-style-type: none"> <li>kps:domainKeypairs:importpk</li> </ul>                                  |
| kps::SSHKeyPair:exportPrivateKey | Grants permission to export the private key of a key pair.    | Write        | SSHKeyPair *                | -             | <ul style="list-style-type: none"> <li>kps:domainKeypairs:exportpk</li> </ul>                                  |
| kps::SSHKeyPair:clearPrivateKey  | Grants permission to clear the private key of a key pair.     | Write        | SSHKeyPair *                | -             | <ul style="list-style-type: none"> <li>kps:domainKeypairs:clearpk</li> </ul>                                   |

Each API of KPS usually supports one or more actions. [Table 3-132](#) lists the supported actions and dependencies.

**Table 3-132** Actions and dependencies supported by KPS APIs

| API                                                         | Action                | Dependencies                                                                                   |
|-------------------------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------|
| POST /v3/<br>{project_id}/<br>keypairs                      | kps:SSHKeyPair:create | <ul style="list-style-type: none"><li>• kms:cmk:createDataKey</li><li>• kms:cmk:list</li></ul> |
| DELETE /v3/<br>{project_id}/<br>keypairs/<br>{keypair_name} | kps:SSHKeyPair:delete | -                                                                                              |
| GET /v3/<br>{project_id}/<br>keypairs/<br>{keypair_name}    | kps:SSHKeyPair:get    | -                                                                                              |
| GET /v3/<br>{project_id}/<br>keypairs                       | kps:SSHKeyPair:list   | -                                                                                              |
| PUT /v3/<br>{project_id}/<br>keypairs/<br>{keypair_name}    | kps:SSHKeyPair:update | -                                                                                              |

| API                                            | Action                | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v3/{project_id}/keypairs/associate       | kps:SSHKeyPair:bind   | <ul style="list-style-type: none"><li>• ecs:cloudServers:createServers</li><li>• ecs:cloudServers:deleteServers</li><li>• ecs:cloudServers:showServer</li><li>• ecs:cloudServers:attach</li><li>• ecs:cloudServers:listServerBlockDevices</li><li>• ecs:cloudServers:showServerBlockDevice</li><li>• ecs:cloudServers:detachVolume</li><li>• ecs:cloudServers:listServerInterfaces</li><li>• ecs:cloudServers:listServersDetails</li><li>• ecs:cloudServerFlavors:get</li><li>• ecs:cloudServerQuotas:get</li><li>• evs:types:get</li><li>• evs:volumes:use</li><li>• ims:images:get</li><li>• vpc:subnets:list</li></ul> |
| DELETE /v3/{project_id}/failed-tasks           | kps::deleteFailedTask | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DELETE /v3/{project_id}/failed-tasks/{task_id} | kps::deleteFailedTask | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| API                                               | Action                          | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v3/{project_id}/keypairs/disassociate       | kps:SSHKeyPair:unbind           | <ul style="list-style-type: none"> <li>ecs:cloudServers:createServers</li> <li>ecs:cloudServers:deleteServers</li> <li>ecs:cloudServers:showServer</li> <li>ecs:cloudServers:attach</li> <li>ecs:cloudServers:listServerBlockDevices</li> <li>ecs:cloudServers:showServerBlockDevice</li> <li>ecs:cloudServers:detachVolume</li> <li>ecs:cloudServers:listServerInterfaces</li> <li>ecs:cloudServers:listServersDetails</li> <li>ecs:cloudServerFlavors:get</li> <li>ecs:cloudServerQuotas:get</li> <li>evs:types:get</li> <li>evs:volumes:use</li> <li>ims:images:get</li> <li>vpc:subnets:list</li> </ul> |
| GET /v3/{project_id}/failed-tasks                 | kps::getFailedTask              | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| GET /v3/{project_id}/tasks/{task_id}              | kps::getTask                    | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| GET /v3/{project_id}/running-tasks                | kps::getRunningTask             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| POST /v3/{project_id}/keypairs/private-key/import | kps:SSHKeyPair:importPrivateKey | <ul style="list-style-type: none"> <li>kms:cmk:createDataKey</li> <li>kms:cmk:list</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| POST /v3/{project_id}/keypairs/private-key/export | kps:SSHKeyPair:exportPrivateKey | kms:cmk:decryptDataKey                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| API                                                         | Action                         | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v3/{project_id}/keypairs/batch-associate              | kps:SSHKeyPair:bind            | <ul style="list-style-type: none"> <li>• ecs:cloudServers:createServers</li> <li>• ecs:cloudServers:deleteServers</li> <li>• ecs:cloudServers:showServer</li> <li>• ecs:cloudServers:attach</li> <li>• ecs:cloudServers:listServerBlockDevices</li> <li>• ecs:cloudServers:showServerBlockDevice</li> <li>• ecs:cloudServers:detachVolume</li> <li>• ecs:cloudServers:listServerInterfaces</li> <li>• ecs:cloudServers:listServersDetails</li> <li>• ecs:cloudServerFlavors:get</li> <li>• ecs:cloudServerQuotas:get</li> <li>• evs:types:get</li> <li>• evs:volumes:use</li> <li>• ims:images:get</li> <li>• vpc:subnets:list</li> </ul> |
| DELETE /v3/{project_id}/keypairs/{keypair_name}/private-key | kps:SSHKeyPair:clearPrivateKey | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-133](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for KPS.

**Table 3-133** Resource types supported by KPS

| Resource Type | URN                                                 |
|---------------|-----------------------------------------------------|
| SSHKeyPair    | kps:<region>:<account-id>:SSHKeyPair:<keypair-name> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, kps) apply only to operations of the xx service. For details, see [Table 3-134](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by KPS

The following table lists the condition keys that you can define in identity policies for KPS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-134** Service-specific condition keys supported by KPS

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                       |
|--------------------------------|--------|-------------------------------|-----------------------------------|
| kps:KmsKeyId                   | string | Single-valued                 | Filters access by the KMS key ID. |

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                          |
|--------------------------------|--------|-------------------------------|--------------------------------------|
| kps:Algorithm                  | string | Single-valued                 | Filters access by SSH key algorithm. |

### 3.7.1.3 Cloud Secret Management Service (CSMS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CSMS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CSMS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CSMS.

**Table 3-135** Actions supported by CSMS

| Action             | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                           | Alias |
|--------------------|---------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| csms:secret:create | Grants permission to create or recover a secret.  | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">csms:KmsKeyId</a></li> </ul>                                                                  | -     |
|                    |                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>  |       |
| csms:secret:delete | Grants permission to delete a secret immediately. | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |



| Action                    | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                    | Alias                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| csms:secret:update        | Grants permission to update the metadata of a secret.                                             | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">csms:KmsKeyId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -                                                                             |
| csms:secret:get           | Grants permission to query or download the secret information.                                    | Read         | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                          | -                                                                             |
| csms:secret:list          | Grants permission to query all the secrets created by the current user under the current project. | List         | secret Name *               | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                            | -                                                                             |
| csms:secret:createVersion | Grants permission to create a secret version in a specified secret.                               | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                          | <ul style="list-style-type: none"> <li>• csms:secretVersion:create</li> </ul> |

| Action                  | Description                                                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                        | Alias                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| csms:secret:getVersion  | Grants permission to query information about a specified secret version and its plaintext secret value. | Read         | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">csms:VersionId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>    | <ul style="list-style-type: none"> <li>• csms:secretVersion:get</li> </ul>  |
| csms:secret:listVersion | Grants permission to list the available versions of a secret.                                           | List         | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                              | <ul style="list-style-type: none"> <li>• csms:secretVersion:list</li> </ul> |
| csms:secret:createStage | Grants permission to create a secret version stage.                                                     | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                              | <ul style="list-style-type: none"> <li>• csms:secretStage:create</li> </ul> |
| csms:secret:getStage    | Grants permission to query version information about a specified secret version stage.                  | Read         | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">csms:VersionStage</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• csms:secretStage:get</li> </ul>    |
| csms:secret:updateStage | Grants permission to update a secret version stage.                                                     | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <a href="#">csms:Type</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                              | <ul style="list-style-type: none"> <li>• csms:secretStage:update</li> </ul> |

| Action                       | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                            | Alias                                                                            |
|------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| csms:secret:deleteStage      | Grants permission to delete a specified secret version stage.       | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <b>csms:Type</b></li> <li>• <b>g:EnterpriseProjectId</b></li> <li>• <b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul>                                             | <ul style="list-style-type: none"> <li>• csms:secret Stage:delete</li> </ul>     |
| csms::getSecretQuota         | Grants permission to query the secret quota of a specified project. | Read         | -                           | -                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• csms:secret Quota:get</li> </ul>        |
| csms:secret:scheduleDeletion | Grants permission to schedule the deletion of a secret.             | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <b>csms:Type</b></li> <li>• <b>csms:RecoveryWindowInDays</b></li> <li>• <b>g:EnterpriseProjectId</b></li> <li>• <b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul> | <ul style="list-style-type: none"> <li>• csms:secret :deleteScheduled</li> </ul> |
| csms:secret:restoreSecret    | Grants permission to cancel the scheduled deletion of a secret.     | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <b>csms:Type</b></li> <li>• <b>g:EnterpriseProjectId</b></li> <li>• <b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul>                                             | <ul style="list-style-type: none"> <li>• csms:secret :deleteCancelled</li> </ul> |
| csms:secret:rotate           | Grants permission to start secret rotation.                         | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <b>csms:Type</b></li> <li>• <b>g:EnterpriseProjectId</b></li> <li>• <b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul>                                             | -                                                                                |

| Action                              | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias                                                                     |
|-------------------------------------|-------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| csms:secret:getSecretsByTag         | Grants permission to list secrets filtered by tags.   | List         | secret Name *               | -                                                                                                                                 | <ul style="list-style-type: none"> <li>csms:tag:getSecretByTag</li> </ul> |
| csms:secret:batchCreateOrDeleteTags | Grants permission to batch add or remove secret tags. | Tagging      | secret Name *               | <ul style="list-style-type: none"> <li>csms:Type</li> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>csms:tag:batch</li> </ul>          |
|                                     |                                                       |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                                 |                                                                           |
| csms:secret:createTag               | Grants permission to add tags to a secret.            | Tagging      | secret Name *               | <ul style="list-style-type: none"> <li>csms:Type</li> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>csms:tag:create</li> </ul>         |
|                                     |                                                       |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                                 |                                                                           |
| csms:secret:deleteTag               | Grants permission to remove tags from a secret.       | Tagging      | secret Name *               | <ul style="list-style-type: none"> <li>csms:Type</li> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | <ul style="list-style-type: none"> <li>csms:tag:delete</li> </ul>         |
|                                     |                                                       |              | -                           | g:TagKeys                                                                                                                         |                                                                           |

| Action                    | Description                                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                 | Alias                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| csms:secret:listTags      | Grants permission to list secret tags.                                                                          | List         | secret Name *               | <ul style="list-style-type: none"> <li>• <b>csms:Type</b></li> <li>• <b>g:EnterpriseProjectId</b></li> <li>• <b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul>                                  | <ul style="list-style-type: none"> <li>• csms:tag:getBySecret</li> </ul>      |
| csms::listProjectTags     | Grants permission to list the secret tags under a specified project.                                            | List         | -                           | -                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• csms:tag:getAll</li> </ul>           |
| csms:secret:updateVersion | Grants permission to update the validity period of a secret version.                                            | Write        | secret Name *               | <ul style="list-style-type: none"> <li>• <b>csms:Type</b></li> <li>• <b>csms:VersionId</b></li> <li>• <b>g:EnterpriseProjectId</b></li> <li>• <b>g:ResourceTag/&lt;tag-key&gt;</b></li> </ul> | <ul style="list-style-type: none"> <li>• csms:secretVersion:update</li> </ul> |
| csms::createEvent         | Grants permission to create a secret event.                                                                     | Write        | -                           | -                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• csms:event:create</li> </ul>         |
| csms::listEvents          | Grants permission to list all secret event notifications created by the current user under the current project. | List         | -                           | -                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• csms:event:list</li> </ul>           |

| Action                        | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                |
|-------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------------------------------------------|
| csms::getEvent                | Grants permission to query a specified secret event notification.                  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>csms:event:get</li> </ul>                     |
| csms::updateEvent             | Grants permission to update the metadata of a specified secret event notification. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>csms:event:update</li> </ul>                  |
| csms::deleteEvent             | Grants permission to immediately delete a specified secret event notification.     | Write        | -                           | -             | <ul style="list-style-type: none"> <li>csms:event:delete</li> </ul>                  |
| csms::listNotificationRecords | Grants permission to list the records about triggered event notifications.         | List         | -                           | -             | <ul style="list-style-type: none"> <li>csms:event:listNotificationRecords</li> </ul> |
| csms::listTasks               | Grants permission to list the secret rotation tasks.                               | List         | -                           | -             | <ul style="list-style-type: none"> <li>csms:task:list</li> </ul>                     |

Each API of CSMS usually supports one or more actions. [Table 3-136](#) lists the supported actions and dependencies.

**Table 3-136** Actions and dependencies supported by CSMS APIs

| API                           | Action             | Dependencies          |
|-------------------------------|--------------------|-----------------------|
| POST /v1/{project_id}/secrets | csms:secret:create | kms:cmk:createDataKey |

| API                                                              | Action                    | Dependencies                                                                                                                  |
|------------------------------------------------------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/{project_id}/secrets/{secret_name}/backup               | csms:secret:get           | <ul style="list-style-type: none"> <li>kms:cmk:createDataKey</li> <li>kms:cmk:decryptDataKey</li> <li>kms:cmk:list</li> </ul> |
| POST /v1/{project_id}/secrets/restore                            | csms:secret:create        | kms:cmk:decryptDataKey                                                                                                        |
| DELETE /v1/{project_id}/secrets/{secret_name}                    | csms:secret:delete        | -                                                                                                                             |
| PUT /v1/{project_id}/secrets/{secret_name}                       | csms:secret:update        | -                                                                                                                             |
| GET /v1/{project_id}/secrets/{secret_name}                       | csms:secret:get           | -                                                                                                                             |
| GET /v1/{project_id}/secrets                                     | csms:secret:list          | -                                                                                                                             |
| POST /v1/{project_id}/secrets/{secret_name}/versions             | csms:secret:createVersion | kms:cmk:createDataKey                                                                                                         |
| GET /v1/{project_id}/secrets/{secret_name}/versions/{version_id} | csms:secret:getVersion    | kms:cmk:decryptDataKey                                                                                                        |
| GET /v1/{project_id}/secrets/{secret_name}/versions              | csms:secret:listVersion   | -                                                                                                                             |
| GET /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}   | csms:secret:getStage      | -                                                                                                                             |
| PUT /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}   | csms:secret:updateStage   | -                                                                                                                             |

| API                                                                        | Action                              | Dependencies                                                                                                                          |
|----------------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v1/{project_id}/secrets/{secret_name}/stages/{stage_name}          | csms:secret:deleteStage             | -                                                                                                                                     |
| POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/create | csms:secret:scheduleDeletion        | -                                                                                                                                     |
| POST /v1/{project_id}/secrets/{secret_name}/scheduled-deleted-tasks/cancel | csms:secret:restoreSecret           | -                                                                                                                                     |
| POST /v1/{project_id}/secrets/{secret_name}/rotate                         | csms:secret:rotate                  | <ul style="list-style-type: none"> <li>• rds:password:update</li> <li>• kms:cmk:createGrant</li> <li>• kms:cmk:retireGrant</li> </ul> |
| POST /v1/{project_id}/csms/{resource_instances}/action                     | csms:secret:getSecretsByTag         | -                                                                                                                                     |
| POST /v1/{project_id}/csms/{secret_id}/tags/action                         | csms:secret:batchCreateOrDeleteTags | -                                                                                                                                     |
| POST /v1/{project_id}/csms/{secret_id}/tags                                | csms:secret:createTag               | -                                                                                                                                     |
| DELETE /v1/{project_id}/csms/{secret_id}/tags/{key}                        | csms:secret:deleteTag               | -                                                                                                                                     |
| GET /v1/{project_id}/csms/{secret_id}/tags                                 | csms:secret:listTags                | -                                                                                                                                     |
| GET /v1/{project_id}/csms/tags                                             | csms::listProjectTags               | -                                                                                                                                     |



| API                                                              | Action                        | Dependencies |
|------------------------------------------------------------------|-------------------------------|--------------|
| PUT /v1/{project_id}/secrets/{secret_name}/versions/{version_id} | csms:secret:updateVersion     | -            |
| POST /v1/{project_id}/csms/events                                | csms::createEvent             | -            |
| GET /v1/{project_id}/csms/events                                 | csms::listEvents              | -            |
| GET /v1/{project_id}/csms/events/{event_name}                    | csms::getEvent                | -            |
| PUT /v1/{project_id}/csms/events/{event_name}                    | csms::updateEvent             | -            |
| DELETE /v1/{project_id}/csms/events/{event_name}                 | csms::deleteEvent             | -            |
| GET /v1/{project_id}/csms/notification-records                   | csms::listNotificationRecords | -            |
| GET /v1/{project_id}/csms/tasks                                  | csms::listTasks               | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-137](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CSMS.

**Table 3-137** Resource types supported by CSMS

| Resource Type | URN                                                 |
|---------------|-----------------------------------------------------|
| secretName    | csms:<region>:<account-id>:secretName:<secret-name> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, csms) apply only to operations of the xx service. For details, see [Table 3-138](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by CSMS

The following table lists the condition keys that you can define in identity policies for CSMS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-138** Service-specific condition keys supported by CSMS

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                    |
|--------------------------------|--------|-------------------------------|--------------------------------|
| csms:Type                      | string | Single-valued                 | Filters access by secret type. |

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                |
|--------------------------------|---------|-------------------------------|--------------------------------------------|
| csms:KmsKeyId                  | string  | Single-valued                 | Filters access by KMS key ID.              |
| csms:VersionId                 | string  | Single-valued                 | Filters access by secret version ID.       |
| csms:VersionStage              | string  | Single-valued                 | Filters access by secret version stage.    |
| csms:RecoveryWindowInDays      | numeric | Single-valued                 | Filters access by scheduled deletion time. |

## 3.7.2 Anti-DDoS Service (AAD)

### 3.7.2.1 Cloud Native Anti-DDoS Basic

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.

- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by Anti-DDoS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Anti-DDoS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Anti-DDoS.

**Table 3-139** Actions supported by Anti-DDoS

| Action                               | Description                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| anti-ddos:task:list                  | Grants permission to query Anti-DDoS tasks.                     | List         | -                           | -             | -     |
| anti-ddos:quota:list                 | Grants permission to query quotas.                              | List         | -                           | -             | -     |
| anti-ddos:optionalDefensePolicy:list | Grants permission to query Anti-DDoS protection specifications. | List         | -                           | -             | -     |

| Action                           | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------|-----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| anti-ddos:logConfig:update       | Grants permission to update LTS configurations.     | Write        | -                           | -                                                                                                                                                  | -     |
| anti-ddos:logConfig:get          | Grants permission to query LTS configurations.      | Read         | -                           | -                                                                                                                                                  | -     |
| anti-ddos:ip:updateDefensePolicy | Grants permission to update Anti-DDoS.              | Write        | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:untagResource       | Grants permission to delete tags in batches.        | Write        | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:tagResource         | Grants permission to add tags in batches.           | Write        | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:listTagsForResource | Grants permission to query resource tags.           | List         | ip *                        | -                                                                                                                                                  | -     |
| anti-ddos:ip:listDefenseStatuses | Grants permission to query EIP protection statuses. | List         | ip *                        | -                                                                                                                                                  | -     |

| Action                             | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| anti-ddos:ip:getWeeklyReport       | Grants permission to query weekly protection statistics.    | Read         | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:getDefenseStatus      | Grants permission to query the protection status of an EIP. | Read         | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:getDefensePolicy      | Grants permission to query Anti-DDoS.                       | Read         | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:getDailyTrafficReport | Grants permission to query protected traffic of an EIP.     | Read         | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:getDailyEventReport   | Grants permission to query abnormal events of an EIP.       | Read         | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:ip:enableDefensePolicy   | Grants permission to enable Anti-DDoS.                      | Write        | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| anti-ddos:ip:disableDefensePolicy     | Grants permission to disable Anti-DDoS.                               | Write        | ip *                        | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| anti-ddos:defaultDefensePolicy:get    | Grants permission to query default Anti-DDoS protection policies.     | Read         | -                           | -                                                                                                                                                  | -     |
| anti-ddos:defaultDefensePolicy:delete | Grants permission to delete default Anti-DDoS protection policies.    | Write        | -                           | -                                                                                                                                                  | -     |
| anti-ddos:defaultDefensePolicy:create | Grants permission to configure default Anti-DDoS protection policies. | Write        | -                           | -                                                                                                                                                  | -     |
| anti-ddos:alertConfig:update          | Grants permission to update alarm configurations.                     | Write        | -                           | -                                                                                                                                                  | -     |
| anti-ddos:alertConfig:get             | Grants permission to query alarm configurations.                      | Read         | -                           | -                                                                                                                                                  | -     |

Each API of Anti-DDoS usually supports one or more actions. [Table 3-140](#) lists the supported actions and dependencies.

**Table 3-140** Actions and dependencies supported by Anti-DDoS APIs

| API                                                           | Action                               | Dependencies |
|---------------------------------------------------------------|--------------------------------------|--------------|
| GET /v2/{project_id}/query-task-status                        | anti-ddos:task:list                  | -            |
| GET /v1/{project_id}/antiddos/quotas                          | anti-ddos:quota:list                 | -            |
| GET /v1/{project_id}/antiddos/query-config-list               | anti-ddos:optionalDefensePolicy:list | -            |
| PUT /v1/{project_id}/antiddos/lts-config                      | anti-ddos:logConfig:update           | -            |
| GET /v1/{project_id}/antiddos/lts-config                      | anti-ddos:logConfig:get              | -            |
| PUT /v1/{project_id}/antiddos/{floating_ip_id}                | anti-ddos:ip:updateDefensePolicy     | -            |
| DELETE /v1/{project_id}/antiddos-ip/{resource_id}/tags/delete | anti-ddos:ip:untagResource           | -            |
| POST /v1/{project_id}/antiddos-ip/{resource_id}/tags/create   | anti-ddos:ip:tagResource             | -            |
| GET /v1/{project_id}/antiddos-ip/{resource_id}/tags           | anti-ddos:ip:listTagsForResource     | -            |
| GET /v1/{project_id}/antiddos-ip/tags                         | anti-ddos:ip:listTagsForResource     | -            |
| GET /v1/{project_id}/antiddos                                 | anti-ddos:ip:listDefenseStatuses     | -            |
| POST /v1/{project_id}/antiddos-ip/resource-instances/count    | anti-ddos:ip:listDefenseStatuses     | -            |
| POST /v1/{project_id}/antiddos-ip/resource-instances/filter   | anti-ddos:ip:listDefenseStatuses     | -            |
| GET /v1/{project_id}/antiddos/weekly                          | anti-ddos:ip:getWeeklyReport         | -            |



| API                                                              | Action                                | Dependencies |
|------------------------------------------------------------------|---------------------------------------|--------------|
| GET /v1/{project_id}/antiddos/weekly-export                      | anti-ddos:ip:getWeeklyReport          | -            |
| GET /v1/{project_id}/antiddos/{floating_ip_id}/status            | anti-ddos:ip:getDefenseStatus         | -            |
| GET /v1/{project_id}/antiddos/{floating_ip_id}                   | anti-ddos:ip:getDefensePolicy         | -            |
| GET /v1/{project_id}/antiddos/queryIsEnabledResult/query         | anti-ddos:ip:getDefensePolicy         | -            |
| GET /v1/{project_id}/antiddos/{floating_ip_id}/daily             | anti-ddos:ip:getDailyTrafficReport    | -            |
| GET /v1/{project_id}/antiddos/{floating_ip_id}/daily-export      | anti-ddos:ip:getDailyTrafficReport    | -            |
| GET /v1/{project_id}/antiddos/{floating_ip_id}/logs              | anti-ddos:ip:getDailyEventReport      | -            |
| POST /v1/{project_id}/antiddos/{floating_ip_id}                  | anti-ddos:ip:enableDefensePolicy      | -            |
| POST /v1/{project_id}/antiddos/immediate_protection              | anti-ddos:ip:enableDefensePolicy      | -            |
| DELETE /v1/{project_id}/antiddos/{floating_ip_id}                | anti-ddos:ip:disableDefensePolicy     | -            |
| DELETE /v1/{project_id}/antiddos/{floating_ip_id}/closeAndReason | anti-ddos:ip:disableDefensePolicy     | -            |
| GET /v1/{project_id}/antiddos/default/config                     | anti-ddos:defaultDefensePolicy:get    | -            |
| DELETE /v1/{project_id}/antiddos/default/config                  | anti-ddos:defaultDefensePolicy:delete | -            |

| API                                                | Action                                | Dependencies |
|----------------------------------------------------|---------------------------------------|--------------|
| POST /v1/{project_id}/antiddos/default/config      | anti-ddos:defaultDefensePolicy:create | -            |
| POST /v2/{project_id}/warnalert/alertconfig/update | anti-ddos:alertConfig:update          | -            |
| GET /v2/{project_id}/warnalert/alertconfig/query   | anti-ddos:alertConfig:get             | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-141](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for Anti-DDoS.

**Table 3-141** Resource types supported by Anti-DDoS

| Resource Type | URN                                        |
|---------------|--------------------------------------------|
| ip            | anti-ddos:<region>:<account-id>:ip:<ip-id> |

## Conditions

Anti-DDoS does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.7.2.2 Cloud Native Anti-DDoS Advanced

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that

OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CNAD, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CNAD, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CNAD.

**Table 3-142** Actions supported by CNAD

| Action                | Description                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------|--------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| cnad:schedule:update  | Grants permission to update scheduling specifications. | Write        | schedule *                  | -             | -     |
| cnad:schedule:list    | Grants permission to query the scheduling rule list.   | List         | schedule *                  | -             | -     |
| cnad:schedule:get     | Grants permission to query scheduling rules.           | Read         | schedule *                  | -             | -     |
| cnad:schedule:delete  | Grants permission to delete scheduling rules.          | Write        | schedule *                  | -             | -     |
| cnad:schedule:create  | Grants permission to create scheduling rules.          | Write        | schedule *                  | -             | -     |
| cnad:quota:update     | Grants permission to modify quotas.                    | Write        | -                           | -             | -     |
| cnad:blockade:release | Grants permission to unblock IP addresses.             | Write        | -                           | -             | -     |
| cnad:blockade:list    | Grants permission to query the blocking list.          | List         | -                           | -             | -     |

| Action                   | Description                                              | Access Level | Resource Type (*: required) | Condition Key | Alias                  |
|--------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------|------------------------|
| cnad:blockade:get        | Grants permission to query blocking records.             | Read         | -                           | -             | -                      |
| cnad:alarmConfig:update  | Grants permission to modify alarm notifications.         | Write        | -                           | -             | -                      |
| cnad:alarmConfig:create  | Grants permission to create alarm notifications.         | Write        | -                           | -             | -                      |
| cnad:alarmConfig:delete  | Grants permission to delete alarm notifications.         | Write        | -                           | -             | -                      |
| cnad:alarmConfig:get     | Grants permission to query alarm notifications.          | Read         | -                           | -             | -                      |
| cnad:attackReport:list   | Grants permission to query attack events.                | List         | -                           | -             | -                      |
| cnad:attackReport:update | Grants permission to update attack event configurations. | Write        | -                           | -             | cnad:attackReport:list |
| cnad:attackTop:list      | Grants permission to query top 10 attacked IP addresses. | List         | -                           | -             | -                      |

| Action                         | Description                                                              | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| cnad:attackTypeReport:list     | Grants permission to query attack type distribution.                     | List         | -                           | -             | -     |
| cnad:bindPolicy:create         | Grants permission to bind protection policies to protected IP addresses. | Write        | -                           | -             | -     |
| cnad:blackWhitelistList:create | Grants permission to create an IP address blacklist or whitelist.        | Write        | -                           | -             | -     |
| cnad:blackWhitelistList:delete | Grants permission to delete an IP address blacklist or whitelist.        | Write        | -                           | -             | -     |
| cnad:cleanCountReport:list     | Grants permission to query the DDoS protection trend.                    | List         | -                           | -             | -     |
| cnad:cleanKbpsReport:list      | Grants permission to query statistics on peak scrubbing traffic.         | List         | -                           | -             | -     |

| Action                       | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cnad:cleanScaleDropList:list | Grants permission to query the scrubbing scope.                 | List         | -                           | -                                                                                                                                                  | -     |
| cnad:countReport:get         | Grants permission to query statistics.                          | Read         | -                           | -                                                                                                                                                  | -     |
| cnad:ipTag:put               | Grants permission to update the tags of protected IP addresses. | Write        | -                           | -                                                                                                                                                  | -     |
| cnad:package:create          | Grants permission to create an instance.                        | Write        | package *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| cnad:package:get             | Grants permission to query an instance.                         | Read         | package *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| cnad:package:list            | Grants permission to query the instance list.                   | List         | package *                   | -                                                                                                                                                  | -     |
| cnad:package:put             | Grants permission to update an instance.                        | Write        | package *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | -     |

| Action                       | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| cnad:packageDropList:list    | Grants permission to query the instance summary list.         | List         | -                           | -                                     | -     |
| cnad:packetAttackReport:list | Grants permission to query attack data packets.               | List         | -                           | -                                     | -     |
| cnad:policy:create           | Grants permission to create protection policies.              | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cnad:policy:delete           | Grants permission to delete protection policies.              | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cnad:policy:get              | Grants permission to query details about a protection policy. | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cnad:policy:list             | Grants permission to query protection policy details.         | List         | policy *                    | -                                     | -     |
| cnad:policy:update           | Grants permission to update protection policies.              | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| cnad:policyDropList:list     | Grants permission to query the protected IP address list.     | List         | -                           | -                                     | -     |



| Action                                | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key | Alias                        |
|---------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------|
| cnad:protecte<br>dlp:create           | Grants permission to bind protected IP addresses to an instance.             | Write        | -                           | -             | -                            |
| cnad:protecte<br>dlp:list             | Grants permission to query the protected IP address list.                    | List         | -                           | -             | -                            |
| cnad:protecte<br>dlpDropList:lis<br>t | Grants permission to query the protected IP address drop list.               | List         | -                           | -             | -                            |
| cnad:quota:ge<br>t                    | Grants permission to query quotas.                                           | Read         | -                           | -             | -                            |
| cnad:securityS<br>tatusReport:ge<br>t | Grants permission to query asset security status.                            | Read         | -                           | -             | -                            |
| cnad:trafficAtt<br>ackReport:list     | Grants permission to query attack traffic.                                   | List         | -                           | -             | -                            |
| cnad:policy:un<br>bind                | Grants permission to remove a protection policy from a protected IP address. | Write        | -                           | -             | cnad:unbindP<br>olicy:create |
| cnad:weekSta<br>tisticsReport:ge<br>t | Grants permission to query weekly security statistics.                       | Read         | -                           | -             | -                            |

Each API of CNAD usually supports one or more actions. [Table 3-143](#) lists the supported actions and dependencies.

**Table 3-143** Actions and dependencies supported by CNAD APIs

| API                                                         | Action                       | Dependencies |
|-------------------------------------------------------------|------------------------------|--------------|
| GET /v1/unblockservice/{domain_id}/unblock-quota-statistics | cnad:quota:get               | -            |
| POST /v1/unblockservice/{domain_id}/unblock                 | cnad:blockade:release        | -            |
| GET /v1/unblockservice/{domain_id}/unblock-record           | cnad:blockade:list           | -            |
| GET /v1/unblockservice/{domain_id}/block-statistics         | cnad:blockade:get            | -            |
| POST /v1/cnad/alarm-config                                  | cnad:alarmConfig:update      | -            |
| DELETE /v1/cnad/alarm-config                                | cnad:alarmConfig:delete      | -            |
| GET /v1/cnad/alarm-config                                   | cnad:alarmConfig:get         | -            |
| POST /v1/cnad/policies/{policy_id}/bind                     | cnad:bindPolicy:create       | -            |
| POST /v1/cnad/policies/{policy_id}/ip-list/add              | cnad:blackWhitelpList:create | -            |
| POST /v1/cnad/policies/{policy_id}/ip-list/delete           | cnad:blackWhitelpList:delete | -            |
| PUT /v1/cnad/protected-ips/tags                             | cnad:ipTag:put               | -            |
| GET /v1/cnad/packages                                       | cnad:package:list            | -            |
| PUT /v1/cnad/packages/{package_id}/name                     | cnad:package:put             | -            |
| POST /v1/cnad/policies                                      | cnad:policy:create           | -            |
| DELETE /v1/cnad/policies/{policy_id}                        | cnad:policy:delete           | -            |
| GET /v1/cnad/policies/{policy_id}                           | cnad:policy:get              | -            |
| GET /v1/cnad/policies                                       | cnad:policy:list             | -            |

| API                                                      | Action                         | Dependencies |
|----------------------------------------------------------|--------------------------------|--------------|
| PUT /v1/cnad/policies/{policy_id}                        | cnad:policy:put                | -            |
| POST /v1/cnad/packages/{package_id}/protected-ips        | cnad:protectedIp:create        | -            |
| GET /v1/cnad/protected-ips                               | cnad:protectedIp:list          | -            |
| GET /v1/cnad/packages/{package_id}/unbound-protected-ips | cnad:protectedIpDrop-List:list | -            |
| POST /v1/cnad/policies/{policy_id}/unbind                | cnad:policy:unbind             | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-144](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CNAD.

**Table 3-144** Resource types supported by CNAD

| Resource Type | URN                                       |
|---------------|-------------------------------------------|
| policy        | cnad::<account-id>:policy:<policy-id>     |
| schedule      | cnad::<account-id>:schedule:<schedule-id> |
| package       | cnad::<account-id>:package:<package-id>   |

## Conditions

CNAD does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.7.2.3 Advanced Anti-DDoS

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by AAD, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by AAD, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for AAD.

**Table 3-145** Actions supported by AAD

| Action                 | Description                                                    | Access Level | Resource Type (*: required) | Condition Key         | Alias |
|------------------------|----------------------------------------------------------------|--------------|-----------------------------|-----------------------|-------|
| aad:alarmConfig:create | Grants permission to create alarm settings.                    | Write        | alarmConfig *               | -                     | -     |
| aad:alarmConfig:put    | Grants permission to modify alarm settings.                    | Write        | alarmConfig *               | -                     | -     |
| aad:alarmConfig:get    | Grants permission to query alarm settings.                     | Read         | alarmConfig *               | -                     | -     |
| aad:alarmConfig:delete | Grants permission to delete alarm settings.                    | Write        | alarmConfig *               | -                     | -     |
| aad:certificate:delete | Grants permission to delete certificates.                      | Write        | certificate *               | -                     | -     |
| aad:certificate:list   | Grants permission to query the certificate list.               | List         | certificate *               | -                     | -     |
| aad:certificate:set    | Grants permission to modify the certificate for a domain name. | Write        | certificate *               | -                     | -     |
|                        |                                                                |              | domain *                    | g:EnterpriseProjectId |       |
| aad:dashboard:delete   | Grants permission to delete report log configurations.         | Write        | -                           | -                     | -     |

| Action            | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|-------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| aad:dashboard:get | Grants permission to obtain report data and log configurations. | Read         | -                           | -                                     | -     |
| aad:dashboard:set | Grants permission to modify report log configurations.          | Write        | -                           | -                                     | -     |
| aad:domain:create | Grants permission to add protected domain names.                | Write        | domain *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:domain:delete | Grants permission to delete protected domain names.             | Write        | domain *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:domain:get    | Grants permission to query domain name details.                 | Read         | domain *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:domain:list   | Grants permission to query the domain name list.                | List         | domain *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:domain:put    | Grants permission to modify domain protection attributes.       | Write        | domain *                    | <a href="#">g:EnterpriseProjectId</a> | -     |

| Action                    | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|---------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| aad:forwardingRule:create | Grants permission to add forwarding rules.                                        | Write        | forwardingRule *            | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:forwardingRule:delete | Grants permission to delete forwarding rules.                                     | Write        | forwardingRule *            | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:forwardingRule:get    | Grants permission to query forwarding rules.                                      | Read         | forwardingRule *            | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:forwardingRule:list   | Grants permission to export forwarding rules.                                     | List         | forwardingRule *            | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:forwardingRule:put    | Grants permission to modify the back-to-source IP address in the forwarding rule. | Write        | forwardingRule *            | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:instance:create       | Grants permission to create an instance.                                          | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:instance:get          | Grants permission to query instance attributes.                                   | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:instance:list         | Grants permission to query the instance list.                                     | List         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |

| Action                      | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|-----------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| aad:instance:put            | Grants permission to modify instance attributes.                     | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:policy:create           | Grants permission to add protection rules.                           | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:policy:delete           | Grants permission to delete protection rules.                        | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:policy:get              | Grants permission to query protection rule details.                  | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:policy:list             | Grants permission to query protection rules.                         | List         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:policy:put              | Grants permission to modify protection rules.                        | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:quotas:get              | Grants permission to query protection specifications.                | Read         | -                           | -                                     | -     |
| aad:whiteBlackIpRule:create | Grants permission to add IP addresses to the blacklist or whitelist. | Write        | whiteBlackIpRule *          | <a href="#">g:EnterpriseProjectId</a> | -     |



| Action                      | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|-----------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| aad:whiteBlackIpRule:delete | Grants permission to delete IP addresses from the blacklist or whitelist. | Write        | whiteBlackIpRule *          | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:whiteBlackIpRule:list   | Grants permission to query the protection blacklist and whitelist.        | List         | whiteBlackIpRule *          | <a href="#">g:EnterpriseProjectId</a> | -     |
| aad:protectedIp:put         | Grants permission to modify tags for protected ip.                        | Write        | -                           | -                                     | -     |
| aad:protectedIp:list        | Grants permission to query the protected ip list.                         | List         | -                           | -                                     | -     |
| aad:package:put             | Grants permission to modify protection package.                           | Write        | package *                   | -                                     | -     |
| aad:package:list            | Grants permission to query the protection package list.                   | List         | package *                   | -                                     | -     |
| aad:block:put               | Grants permission to unblock ip.                                          | Write        | -                           | -                                     | -     |
| aad:block:list              | Grants permission to query the blocked ip list.                           | List         | -                           | -                                     | -     |

| Action        | Description                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| aad:block:get | Grants permission to query the blocking and unblocking information. | Read         | -                           | -             | -     |

Each API of AAD usually supports one or more actions. [Table 3-146](#) lists the supported actions and dependencies.

**Table 3-146** Actions and dependencies supported by AAD APIs

| API                                              | Action                 | Dependencies |
|--------------------------------------------------|------------------------|--------------|
| POST /v1/{project_id}/cad/alart/config           | aad:alarmConfig:create | -            |
| POST /v1/cnad/alarm-config                       | aad:alarmConfig:put    | -            |
| DELETE /v1/cnad/alarm-config                     | aad:alarmConfig:delete | -            |
| GET /v1/{project_id}/cad/alart/list              | aad:alarmConfig:get    | -            |
| GET /v1/cnad/alarm-config                        | aad:alarmConfig:get    | -            |
| DELETE /v1/aad/certificate/del                   | aad:certificate:delete | -            |
| GET /v1/{project_id}/cad/domains/certificatelist | aad:certificate:list   | -            |
| GET /v1/aad/certificate-details                  | aad:certificate:list   | -            |
| POST /v1/{project_id}/cad/domains/certificate    | aad:certificate:set    | -            |
| POST /v1/aad/configs/lts/delete                  | aad:dashboard:delete   | -            |
| GET /v1/{project_id}/cad/ddosinfo/events_type    | aad:dashboard:get      | -            |
| GET /v1/aad/configs/lts_region                   | aad:dashboard:get      | -            |
| GET /v1/aad/configs/lts                          | aad:dashboard:get      | -            |
| GET /v1/{project_id}/waf/event/timeline          | aad:dashboard:get      | -            |

| API                                                           | Action            | Dependencies |
|---------------------------------------------------------------|-------------------|--------------|
| GET /v1/{project_id}/waf/event/request/peak                   | aad:dashboard:get | -            |
| GET /v1/{project_id}/waf/event/attack/type                    | aad:dashboard:get | -            |
| GET /v1/{project_id}/waf/event/attack/source/num              | aad:dashboard:get | -            |
| GET /v1/{project_id}/waf/event/attack/source                  | aad:dashboard:get | -            |
| GET /v1/{project_id}/cad/instances/flow_pps                   | aad:dashboard:get | -            |
| GET /v1/{project_id}/cad/instances/flow_bps                   | aad:dashboard:get | -            |
| GET /v1/{project_id}/cad/instances/events                     | aad:dashboard:get | -            |
| GET /v1/{project_id}/cad/ddosinfo/peak                        | aad:dashboard:get | -            |
| POST /v1/aad/configs/lts                                      | aad:dashboard:set | -            |
| POST /v1/{project_id}/aad/domains                             | aad:domain:create | -            |
| POST /v1/{project_id}/cad/domains/del                         | aad:domain:delete | -            |
| GET /v1/{project_id}/aad/domains/{domain_id}/service-config   | aad:domain:get    | -            |
| GET /v1/{project_id}/cad/domains/ports                        | aad:domain:list   | -            |
| GET /v1/{project_id}/cad/domains/name                         | aad:domain:get    | -            |
| GET /v1/{project_id}/cad/domains/line/{enterprise_project_id} | aad:domain:list   | -            |
| GET /v1/{project_id}/cad/domains/instances                    | aad:domain:get    | -            |
| GET /v1/{project_id}/cad/domains/brief                        | aad:domain:get    | -            |
| GET /v1/{project_id}/aad/domains/waf-list                     | aad:domain:list   | -            |

| API                                                           | Action                    | Dependencies |
|---------------------------------------------------------------|---------------------------|--------------|
| GET /v1/{project_id}/cad/domains                              | aad:domain:list           | -            |
| POST /v1/{project_id}/aad/domains/{domain_id}/service-config  | aad:domain:put            | -            |
| POST /v1/{project_id}/cad/domains/switch                      | aad:domain:put            | -            |
| POST /v1/{project_id}/cad/domains/cnameDispatchSwitch         | aad:domain:put            | -            |
| POST /v1/{project_id}/cad/domains/cname/switch                | aad:domain:put            | -            |
| POST /v1/{project_id}/cad/instances/protocol_rule             | aad:forwardingRule:create | -            |
| POST /v1/{project_id}/cad/instances/protocol_rule/import      | aad:forwardingRule:create | -            |
| DELETE /v1/{project_id}/cad/instances/protocol_rule/{rule_id} | aad:forwardingRule:delete | -            |
| POST /v1/{project_id}/cad/instances/protocol_rule/batchdel    | aad:forwardingRule:delete | -            |
| GET /v1/{project_id}/cad/instances/rules                      | aad:forwardingRule:get    | -            |
| GET /v1/{project_id}/cad/instances/protocol_rule/export       | aad:forwardingRule:list   | -            |
| PUT /v1/{project_id}/cad/instances/protocol_rule/{rule_id}    | aad:forwardingRule:put    | -            |
| POST /v1/{project_id}/cad/instances/cad_open                  | aad:instance:create       | -            |
| GET /v1/{project_id}/cad/products                             | aad:instance:create       | -            |
| GET /v1/{project_id}/{resource_type}/{resource_id}/tags       | aad:instance:get          | -            |
| GET /v1/{project_id}/cad/upgradeproducts/{instance_id}        | aad:instance:get          | -            |
| GET /v1/{project_id}/cad/instances/detail/{instance_id}       | aad:instance:get          | -            |
| GET /v1/{project_id}/aad/instances/brief-list                 | aad:instance:list         | -            |

| API                                                              | Action            | Dependencies |
|------------------------------------------------------------------|-------------------|--------------|
| GET /v1/{project_id}/cad/sourceip                                | aad:instance:list | -            |
| GET /v1/{project_id}/cad/instances                               | aad:instance:list | -            |
| POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action  | aad:instance:put  | -            |
| POST /v1/{project_id}/cad/instances/cad_spec_upgrade             | aad:instance:put  | -            |
| PUT /v1/{project_id}/cad/instances/{instance_id}/name            | aad:instance:put  | -            |
| PUT /v1/{project_id}/cad/instances/{instance_id}/elastic/{ip_id} | aad:instance:put  | -            |
| POST /v1/{project_id}/aad/policies/waf/cc                        | aad:policy:create | -            |
| POST /v1/cnad/policies                                           | aad:policy:create | -            |
| DELETE /v1/{project_id}/aad/policies/waf/cc/{rule_id}            | aad:policy:delete | -            |
| DELETE /v1/cnad/policies/{policy_id}                             | aad:policy:delete | -            |
| GET /v1/{project_id}/cad/flowblock                               | aad:policy:get    | -            |
| GET /v1/cnad/policies/{policy_id}                                | aad:policy:get    | -            |
| GET /v1/{project_id}/aad/policies/waf/cc                         | aad:policy:list   | -            |
| GET /v1/cnad/policies                                            | aad:policy:list   | -            |
| PUT /v1/{project_id}/aad/policies/waf/cc/{rule_id}               | aad:policy:put    | -            |
| POST /v1/{project_id}/cad/flowblock/udp                          | aad:policy:put    | -            |
| POST /v1/{project_id}/cad/flowblock/foreign                      | aad:policy:put    | -            |
| POST /v1/cnad/policies/{policy_id}/ip-list/add                   | aad:policy:put    | -            |
| POST /v1/cnad/policies/{policy_id}/bind                          | aad:policy:put    | -            |

| API                                                      | Action                      | Dependencies |
|----------------------------------------------------------|-----------------------------|--------------|
| POST /v1/cnad/policies/{policy_id}/ip-list/delete        | aad:policy:put              | -            |
| POST /v1/cnad/policies/{policy_id}/unbind                | aad:policy:put              | -            |
| PUT /v1/cnad/policies/{policy_id}                        | aad:policy:put              | -            |
| GET /v1/{project_id}/aad/quotas/domain-port              | aad:quotas:get              | -            |
| GET /v1/{project_id}/scc/waf/quota                       | aad:quotas:get              | -            |
| GET /v1/{project_id}/cad/quotas                          | aad:quotas:get              | -            |
| GET /v1/{project_id}/cad/ip/quotas                       | aad:quotas:get              | -            |
| GET /v1/{project_id}/cad/bwlist/quota                    | aad:quotas:get              | -            |
| GET /v1/{project_id}/aad/user-configs                    | aad:quotas:get              | -            |
| POST /v1/{project_id}/cad/bwlist                         | aad:whiteBlackIpRule:create | -            |
| POST /v1/{project_id}/cad/bwlist/delete                  | aad:whiteBlackIpRule:delete | -            |
| GET /v1/{project_id}/cad/bwlist                          | aad:whiteBlackIpRule:list   | -            |
| PUT /v1/cnad/protected-ips/tags                          | aad:protectedIp:put         | -            |
| GET /v1/cnad/protected-ips                               | aad:protectedIp:list        | -            |
| POST /v1/cnad/packages/{package_id}/protected-ips        | aad:package:put             | -            |
| PUT /v1/cnad/packages/{package_id}/name                  | aad:package:put             | -            |
| GET /v1/cnad/packages                                    | aad:package:list            | -            |
| GET /v1/cnad/packages/{package_id}/unbound-protected-ips | aad:package:list            | -            |
| POST /v1/unblockservice/{domain_id}/unblock              | aad:block:put               | -            |
| GET /v1/unblockservice/{domain_id}/block-list            | aad:block:list              | -            |

| API                                                                     | Action            | Dependencies |
|-------------------------------------------------------------------------|-------------------|--------------|
| GET /v1/unblockservice/{domain_id}/unblock-quota-statistics             | aad:block:get     | -            |
| GET /v1/unblockservice/{domain_id}/block-statistics                     | aad:block:get     | -            |
| GET /v1/unblockservice/{domain_id}/unblock-record                       | aad:block:get     | -            |
| GET /v1/{project_id}/cad/instances/{instance_id}/elastic_count/{ip_id}  | aad:instance:get  | -            |
| GET /v1/{project_id}/cad/instances/{data_center}/elastic/{line}/{ip_id} | aad:instance:get  | -            |
| GET /v1/aad/remain-vip-number                                           | aad:quotas:get    | -            |
| GET /v1/aad/instance/connection-num                                     | aad:dashboard:get | -            |
| PUT /v1/{project_id}/cad/instances/{instance_id}/pp-switch              | aad:instance:put  | -            |
| GET /v1/aad-service/ces/{domain_id}/dims-info                           | aad:instance:list | -            |
| GET /v1/aad-service/ces/v2/{domain_id}/instances                        | aad:instance:list | -            |
| GET /v1/{project_id}/cad/instances/security-statistics                  | aad:instance:list | -            |
| GET /v1/aad/domain/instances/rules                                      | aad:domain:list   | -            |
| POST /v1/aad/policy/modify                                              | aad:policy:put    | -            |
| POST /v1/aad/geoip                                                      | aad:policy:put    | -            |
| GET /v1/aad/geoip                                                       | aad:policy:get    | -            |
| DELETE /v1/aad/geoip/{ruleId}                                           | aad:policy:delete | -            |
| PUT /v1/aad/geoip/{ruleId}                                              | aad:policy:put    | -            |
| POST /v1/aad/whiteip                                                    | aad:policy:put    | -            |
| GET /v1/aad/whiteip                                                     | aad:policy:get    | -            |
| DELETE /v1/aad/whiteip                                                  | aad:policy:delete | -            |
| POST /v1/aad/custom                                                     | aad:policy:put    | -            |

| API                                | Action            | Dependencies |
|------------------------------------|-------------------|--------------|
| GET /v1/aad/custom                 | aad:policy:get    | -            |
| PUT /v1/aad/custom/{ruleId}        | aad:policy:put    | -            |
| DELETE /v1/aad/custom/{ruleId}     | aad:policy:delete | -            |
| GET /v1/aad/policy/details         | aad:policy:get    | -            |
| POST /v1/aad/cc/intelligent/modify | aad:policy:put    | -            |
| GET /v1/aad/geoip/map              | aad:policy:get    | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-147](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for AAD.

**Table 3-147** Resource types supported by AAD

| Resource Type    | URN                                                         |
|------------------|-------------------------------------------------------------|
| forwardingRule   | aad::<account-id>:forwardingRule:<forwarding-rule-id>       |
| package          | aad::<account-id>:package:<package-id>                      |
| policy           | aad::<account-id>:policy:<policy-id>                        |
| alarmConfig      | aad::<account-id>:alarmConfig:<alarm-config-id>             |
| domain           | aad::<account-id>:domain:<domain-id>                        |
| certificate      | aad::<account-id>:certificate:<certificate-id>              |
| instance         | aad::<account-id>:instance:<instance-id>                    |
| whiteBlackIpRule | aad::<account-id>:whiteBlackIpRule:<white-black-ip-rule-id> |

## Conditions

AAD does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).



### 3.7.3 Cloud Firewall (CFW)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CFW, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CFW, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CFW.

**Table 3-148** Actions supported by CFW

| Action                              | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias            |
|-------------------------------------|-------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| cfw:acl:createAclRule               | Grants permission to create an acl rule.        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:acl:create |
| cfw:acl:deleteAclRule               | Grants permission to delete an acl rule.        | Write        | acl *                       | -                                                                                                                                                  | • cfw:acl:delete |
|                                     |                                                 |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                  |
| cfw:acl:deleteHitCount              | Grants permission to delete acl rule hit count. | Write        | acl *                       | -                                                                                                                                                  | • cfw:acl:list   |
|                                     |                                                 |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                  |
| cfw:instance:listDomainParseServers | Grants permission to get domain parse server.   | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:domain:get |

| Action                            | Description                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                              |
|-----------------------------------|-----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| cfw:instance:getDomainParseResult | Grants permission to parse domain.            | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:domain:get</li> </ul> |
| cfw:acl:getExportStatus           | Grants permission to get acl export status.   | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:acl:list</li> </ul>   |
| cfw:acl:getImportStatus           | Grants permission to get acl import status.   | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:acl:list</li> </ul>   |
| cfw:acl:getImportTemplate         | Grants permission to get acl import template. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:acl:list</li> </ul>   |
| cfw:acl:listAclRules              | Grants permission to list acl rules.          | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:acl:list</li> </ul>   |
| cfw:acl:listAclTags               | Grants permission to list acl rule tags.      | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:acl:list</li> </ul>   |

| Action                               | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|--------------------------------------|--------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| cfw:acl:updateAclRule                | Grants permission to update acl rule.            | Write        | acl *                       | -                                                                                                                                                  | • cfw:acl:put           |
|                                      |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                         |
| cfw:acl:updateAclRuleAction          | Grants permission to update acl rule action.     | Write        | acl *                       | -                                                                                                                                                  | • cfw:acl:put           |
|                                      |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                         |
| cfw:instance:updateDomainParseServer | Grants permission to update domain parse server. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:acl:put           |
| cfw:acl:setPriority                  | Grants permission to set acl rule priority.      | Write        | acl *                       | -                                                                                                                                                  | -                       |
|                                      |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                         |
| cfw:blackWhiteList:create            | Grants permission to create blackwhite list.     | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:blackWhite:create |
| cfw:blackWhiteList:delete            | Grants permission to delete blackwhite list.     | Write        | blackWhiteList *            | -                                                                                                                                                  | • cfw:blackWhite:delete |

| Action                    | Description                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|---------------------------|----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                           |                                              |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                       |
| cfw:blackWhiteList:list   | Grants permission to list blackwhite lists.  | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:blackWhite:list |
| cfw:blackWhiteList:update | Grants permission to update blackwhite list. | Write        | blackWhiteList *            | -                                                                                                                                                  | • cfw:blackWhite:put  |
|                           |                                              |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                       |
| cfw:domainGroup:update    | Grants permission to update domainGroup.     | Write        | domainGroup *               | -                                                                                                                                                  | • cfw:ipGroup:put     |
|                           |                                              |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                       |
| cfw:domainGroup:create    | Grants permission to create domainGroup.     | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:ipGroup:create  |

| Action                           | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                   |
|----------------------------------|--------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| cfw:domainGroup:delete           | Grants permission to delete domainGroup.         | Write        | domainGroup *               | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipGroup:delete</li> </ul>    |
|                                  |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                         |
| cfw:domainGroup:list             | Grants permission to list domainGroup.           | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:ipGroup:list</li> </ul>      |
| cfw:eip:count                    | Grants permission to get eip statistics.         | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:eipStatistics:get</li> </ul> |
| cfw:eip:list                     | Grants permission to list eip.                   | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | -                                                                       |
| cfw:eip:updateProtectStatus      | Grants permission to change eip protect status.  | Write        | eip *                       | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:eip:operate</li> </ul>       |
|                                  |                                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          |                                                                         |
| cfw:instance:checkNameRepeat     | Grants permission to check if cfw name repeat.   | Read         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:instance:list</li> </ul>     |
| cfw:instance:listAdvanceIpsRules | Grants permission to list cfw advance ips rules. | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:ipsMode:get</li> </ul>       |

| Action                              | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                  |
|-------------------------------------|---------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| cfw:instance:listUsedEr             | Grants permission to list used er.                      | List         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:instance:list</li> </ul>    |
| cfw:instance:listUsedInspectionVpc  | Grants permission to list used vpc.                     | List         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:instance:list</li> </ul>    |
| cfw:instance:addLogConfig           | Grants permission to add CFW log config.                | Write        | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:instance:create</li> </ul>  |
|                                     |                                                         |              | -                           | <a href="#">cfw:LogGroupId</a>                                                                                                                 |                                                                        |
| cfw:instance:updateCustomRule       | Grants permission to update CFW custom ips rule.        | Write        | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:ipsMode:operate</li> </ul>  |
| cfw:instance:updateCustomRuleAction | Grants permission to update CFW custom ips rule action. | Write        | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:ipsMode:operate</li> </ul>  |
| cfw:instance:updateLogConfig        | Grants permission to update CFW LTS log config.         | Write        | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:instance:upgrade</li> </ul> |
|                                     |                                                         |              | -                           | <a href="#">cfw:LogGroupId</a>                                                                                                                 |                                                                        |
| cfw:instance:createInstance         | Grants permission to create an CFW instance.            | Write        | instance *                  | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:instance:create</li> </ul>  |

| Action                              | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                    |
|-------------------------------------|-----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                                     |                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                          |
| cfw:instance:deletePostPaidInstance | Grants permission to delete post paid CFW instance. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -                        |
| cfw:instance:createCaptureTask      | Grants permission to create CFW capture task.       | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | • cfw:captureTask:create |
| cfw:instance:createCustomRule       | Grants permission to create CFW custom rule.        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | • cfw:ipsMode:operate    |
| cfw:instance:createTags             | Grants permission to create CFW tags.               | Tagging      | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | • cfw:instance:upgrade   |
|                                     |                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                  |                          |



| Action                              | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                       |
|-------------------------------------|-----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| cfw:instance:deleteInstance         | Grants permission to delete CFW instance.           | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:instance:delete       |
| cfw:instance:deleteCaptureTask      | Grants permission to delete CFW capture task.       | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:captureTask:delete    |
| cfw:instance:deleteCustomRule       | Grants permission to delete CFW custom ips rule.    | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:ipsMode:operate       |
| cfw:instance:deleteLogSearchHistory | Grants permission to delete CFW log search history. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:ipsMode:operate       |
| cfw:instance:deleteTags             | Grants permission to delete CFW tags.               | Tagging      | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:instance:upgrade      |
|                                     |                                                     |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |                             |
| cfw:instance:exportLog              | Grants permission to export log.                    | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:accessControlLog:list |

| Action                                  | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                     |
|-----------------------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| cfw:instance:listInstanceByTags         | Grants permission to list cfw by tags.                   | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | cfw:instance:list         |
|                                         |                                                          |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                          |                           |
| cfw:instance:getBaseVersion             | Grants permission to get cfw base version.               | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | cfw:baseVersion:get       |
| cfw:instance:getCaptureTaskResult       | Grants permission to get cfw capture task result.        | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | cfw:captureTask:getResult |
| cfw:instance:getCustomRule              | Grants permission to get cfw custom rule.                | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | cfw:ipsMode:get           |
| cfw:instance:getDomainParseServerStatus | Grants permission to get cfw domain parse server status. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | cfw:domain:get            |
| cfw:instance:getIpsMode                 | Grants permission to get cfw ips mode.                   | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | cfw:ipsMode:get           |

| Action                              | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                        |
|-------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| cfw:instance:getIpsStatus           | Grants permission to get cfw ips status.                     | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:ipsStatus:get</li> </ul>        |
| cfw:instance:getLogConfig           | Grants permission to get cfw log config.                     | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:attackLog:list</li> </ul>       |
| cfw:instance:getMaxCapturePacketNum | Grants permission to get cfw user max capture packet number. | Read         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• cfw:captureTask:list</li> </ul>     |
| cfw:instance:getPolicyStatistics    | Grants permission to get cfw policy statistics.              | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:policyStatistics:get</li> </ul> |
| cfw:instance:listProjectTags        | Grants permission to list project tags.                      | List         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• cfw:instance:list</li> </ul>        |
| cfw:instance:getRegionDb            | Grants permission to get cfw region db.                      | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:acl:list</li> </ul>             |
| cfw:instance:listInstanceTags       | Grants permission to list cfw tags.                          | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:instance:list</li> </ul>        |

| Action                            | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                       |
|-----------------------------------|---------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| cfw:instance:listInstance         | Grants permission to list CFW instances.          | List         | instance *                  | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:instance:list</li> </ul>         |
| cfw:instance:getInstance          | Grants permission to get CFW instances detail.    | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:instance:list</li> </ul>         |
| cfw:instance:listAccessControlLog | Grants permission to list CFW access control log. | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:accessControlLog:list</li> </ul> |
| cfw:instance:listAttackLog        | Grants permission to list CFW attack log.         | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:attackLog:list</li> </ul>        |
| cfw:instance:listCaptureTask      | Grants permission to list CFW capture tasks.      | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:captureTask:list</li> </ul>      |
| cfw:instance:listCustomRule       | Grants permission to list CFW custom ips rule.    | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:ipsMode:get</li> </ul>           |

| Action                            | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                   |
|-----------------------------------|---------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| cfw:instance:getEw                | Grants permission to get cfw east-west firewall.  | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:instance:list</li> </ul>   |
| cfw:instance:listFlowLog          | Grants permission to list cfw flow log.           | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:flowLog:list</li> </ul>    |
| cfw:instance:listIpsRule          | Grants permission to list cfw ips rules.          | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:ipsMode:get</li> </ul>     |
| cfw:instance:listProtectedVpc     | Grants permission to list cfw protect vpcs.       | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:instance:list</li> </ul>   |
| cfw:instance:updateIpsMode        | Grants permission to update cfw ips mode.         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:ipsMode:operate</li> </ul> |
| cfw:instance:updateAdvanceIpsRule | Grants permission to update cfw advance ips rule. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:ipsMode:operate</li> </ul> |

| Action                               | Description                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|--------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| cfw:instance:updateIpsRuleAction     | Grants permission to update cfw ips rule mode.                     | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:ipsMode:operate   |
| cfw:instance:updateIpsStatus         | Grants permission to update cfw ips status.                        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:ipsMode:operate   |
| cfw:instance:updateEwProtectedStatus | Grants permission to update cfw east-west firewall protect status. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:instance:create   |
| cfw:instance:saveTags                | Grants permission to save cfw tags.                                | Tagging      | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:instance:upgrade  |
|                                      |                                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                         |
| cfw:instance:startBaseVersion        | Grants permission to start cfw base version.                       | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • cfw:baseVersion:start |

| Action                         | Description                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                    |
|--------------------------------|-----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| cfw:instance:stopBaseVersion   | Grants permission to stop cfw base version.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:baseVersion:stop</li> </ul> |
| cfw:instance:stopCaptureTask   | Grants permission to stop cfw capture task.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:captureTask:stop</li> </ul> |
| cfw:instance:updateAlarmConfig | Grants permission to update cfw alarm config. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:instance:create</li> </ul>  |
| cfw:instance:getAlarmConfig    | Grants permission to get cfw alarm config.    | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:instance:list</li> </ul>    |
| cfw:instance:upgradeInstance   | Grants permission to upgrade cfw.             | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:instance:upgrade</li> </ul> |
| cfw:instance:updateName        | Grants permission to update cfw name.         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:instance:upgrade</li> </ul> |

| Action                                     | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                              |
|--------------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| cfw:instance:getAccessControlLogStatistics | Grants permission to get cfw access control log statistics. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:accessControlLogReport:get</li> </ul> |
| cfw:instance:getAttackLogStatistics        | Grants permission to get cfw attack log statistics.         | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:attackLogReport:get</li> </ul>        |
| cfw:instance:getLogSearchHistory           | Grants permission to get cfw log search history.            | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:attackLogReport:get</li> </ul>        |
| cfw:instance:getEngineLogStatistics        | Grants permission to get cfw engine log statistics.         | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:attackLogReport:get</li> </ul>        |
| cfw:instance:getFlowLogStatistics          | Grants permission to get cfw flow log statistics.           | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:flowLogReport:get</li> </ul>          |
| cfw:instance:getIpLogStatistics            | Grants permission to get cfw ip log statistics.             | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• cfw:attackLogReport:get</li> </ul>        |



| Action                          | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                 |
|---------------------------------|--------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| cfw:ipGroup:updateIpGroupMember | Grants permission to update cfw ip group member. | Write        | ipGroup *                   | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipMember:put</li> </ul>    |
|                                 |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                       |
| cfw:ipGroup:createIpGroup       | Grants permission to change cfw ip group member. | Write        | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | cfw:ipGroup:create                                                    |
| cfw:ipGroup:createIpGroupMember | Grants permission to create cfw ip group member. | Write        | ipGroup *                   | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipMember:create</li> </ul> |
|                                 |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                       |
| cfw:ipGroup:deleteIpGroup       | Grants permission to delete cfw ip group.        | Write        | ipGroup *                   | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipGroup:delete</li> </ul>  |
|                                 |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                       |
| cfw:ipGroup:deleteIpGroupMember | Grants permission to delete cfw ip group member. | Write        | ipGroup *                   | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipMember:delete</li> </ul> |
|                                 |                                                  |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                       |

| Action                                    | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                   |
|-------------------------------------------|-------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| cfw:ipGroup:getIpGroup                    | Grants permission to get cfw ip group.                | Read         | ipGroup *                   | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipGroup:get</li> </ul>       |
|                                           |                                                       |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                         |
| cfw:ipGroup:listIpGroups                  | Grants permission to list cfw ip groups.              | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>cfw:ipGroup:list</li> </ul>      |
| cfw:ipGroup:listIpGroupMember             | Grants permission to list cfw ip group members.       | List         | ipGroup *                   | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipMember:list</li> </ul>     |
|                                           |                                                       |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                         |
| cfw:ipGroup:updateIpGroup                 | Grants permission to update cfw ip group.             | Write        | ipGroup *                   | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:ipGroup:put</li> </ul>       |
|                                           |                                                       |              | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                         |
| cfw:serviceGroup:updateServiceGroupMember | Grants permission to update cfw service group member. | Write        | serviceGroup *              | -                                                                                                                                              | <ul style="list-style-type: none"> <li>cfw:serviceMember:put</li> </ul> |

| Action                                    | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                        |
|-------------------------------------------|-------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
|                                           |                                                       |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                              |
| cfw:serviceGroup:create                   | Grants permission to create cfw service group member. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                            |
| cfw:serviceGroup:createServiceGroupMember | Grants permission to create cfw service group member. | Write        | serviceGroup *              | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• cfw:serviceMember:create</li> </ul> |
|                                           |                                                       |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                              |
| cfw:serviceGroup:delete                   | Grants permission to delete cfw service group.        | Write        | serviceGroup *              | -                                                                                                                                                  | -                                                                            |
|                                           |                                                       |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                              |
| cfw:serviceGroup:deleteServiceGroupMember | Grants permission to delete cfw service group member. | Write        | serviceGroup *              | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• cfw:serviceMember:delete</li> </ul> |
|                                           |                                                       |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                              |

| Action                                  | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                      |
|-----------------------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| cfw:serviceGroup:get                    | Grants permission to get cfw service group.          | Read         | serviceGroup *              | -                                                                                                                                                  | -                                                                          |
|                                         |                                                      |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                            |
| cfw:serviceGroup:list                   | Grants permission to list cfw service groups.        | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                          |
| cfw:serviceGroup:listServiceGroupMember | Grants permission to list cfw service group members. | List         | serviceGroup *              | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• cfw:serviceMember:list</li> </ul> |
|                                         |                                                      |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                            |
| cfw:serviceGroup:update                 | Grants permission to update cfw service group.       | Write        | serviceGroup *              | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• cfw:serviceGroup:put</li> </ul>   |
|                                         |                                                      |              | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                            |
| cfw:instance:enableMultiAccount         | Grants permission to enable multi account.           | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                          |

| Action                            | Description                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------------------|----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cfw:instance:listAccounts         | Grants permission to list accounts.          | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:listOrganizationTree | Grants permission to list organization tree. | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:addAccount           | Grants permission to add account.            | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:deleteAccount        | Grants permission to delete account.         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:getProtectedVpc      | Grants permission to get protected vpc.      | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:deleteProtectedVpc   | Grants permission to delete protected vpc.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                             | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cfw:instance:addProtectedVpc       | Grants permission to add protected vpc.            | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:updateProtectedVpc    | Grants permission to update protected vpc.         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:updateAntiVirusStatus | Grants permission to update cfw anti virus status. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:getAntiVirusStatus    | Grants permission to get cfw anti virus status.    | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:updateAntiVirusRule   | Grants permission to update cfw anti virus rule.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:getAntiVirusRule      | Grants permission to get cfw anti virus rule.      | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                           | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cfw:instance:listReportProfile   | Grants permission to list cfw report profile rules.  | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:createReportProfile | Grants permission to create cfw report profile rule. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:updateReportProfile | Grants permission to update cfw report profile rule. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:getReportProfile    | Grants permission to show cfw report profile rule.   | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:deleteReportProfile | Grants permission to delete cfw report profile rule. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:importCertificate   | Grants permission to import tls certificate.         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                         | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------|-------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cfw:instance:getCertificate    | Grants permission to get tls certificate information. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| cfw:instance:deleteCertificate | Grants permission to delete tls certificate.          | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

Each API of CFW usually supports one or more actions. [Table 3-149](#) lists the supported actions and dependencies.

**Table 3-149** Actions and dependencies supported by CFW APIs

| API                                          | Action                            | Dependencies |
|----------------------------------------------|-----------------------------------|--------------|
| GET /v1/{project_id}/cfw/logs/flow           | cfw:instance:listFlowLog          | -            |
| GET /v1/{project_id}/cfw/logs/access-control | cfw:instance:listAccessControlLog | -            |
| GET /v1/{project_id}/cfw/logs/attack         | cfw:instance:listAttackLog        | -            |
| PUT /v1/{project_id}/cfw/logs/configuration  | cfw:instance:updateLogConfig      | -            |
| GET /v1/{project_id}/acl-rule/import-status  | cfw:acl:getImportStatus           | -            |



| API                                                | Action                             | Dependencies                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/{project_id}/firewall/east-west           | cfw:instance:createInstance        | <ul style="list-style-type: none"> <li>er:instances:list</li> <li>er:instances:listVpcAttachments</li> <li>er:attachments:create</li> <li>vpc:vpcs:list</li> <li>vpc:subnets:get</li> <li>vpc:subnets:create</li> <li>vpc:routeTables:list</li> <li>vpc:routeTables:update</li> <li>vpc:quotas:list</li> <li>nat:natGateways:list</li> </ul> |
| DELETE /v2/{project_id}/firewall/{resource_id}     | cfw:instance:deleteInstance        | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v1/{project_id}/ips-rule                      | cfw:instance:listIpsRule           | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v1/{project_id}/regions                       | cfw:instance:getRegionDb           | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v1/{project_id}/advanced-ips-rules            | cfw:instance:listAdvancedIpsRules  | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v1/{project_id}/advanced-ips-rule            | cfw:instance:updateAdvancedIpsRule | -                                                                                                                                                                                                                                                                                                                                            |
| GET /v1/{project_id}/ips/custom-rule               | cfw:instance:listCustomRule        | -                                                                                                                                                                                                                                                                                                                                            |
| PUT /v1/{project_id}/ips/custom-rule/{ips_cfw_id}  | cfw:instance:updateCustomRule      | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v1/{project_id}/ips/custom-rule/batch-delete | cfw:instance:deleteCustomRule      | -                                                                                                                                                                                                                                                                                                                                            |
| POST /v1/{project_id}/ips/custom-rule              | cfw:instance:createCustomRule      | -                                                                                                                                                                                                                                                                                                                                            |

| API                                                          | Action                         | Dependencies                                                                                                                                                                                              |
|--------------------------------------------------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1/{project_id}/cfw/alarm/config                        | cfw:instance:getAlarmConfig    | -                                                                                                                                                                                                         |
| PUT /v1/{project_id}/cfw/alarm/config                        | cfw:instance:updateAlarmConfig | -                                                                                                                                                                                                         |
| GET /v1/{project_id}/firewall/east-west                      | cfw:instance:getEw             | <ul style="list-style-type: none"> <li>er:instances:listVpcAttachments</li> <li>vpc:vpcs:list</li> <li>nat:natGateways:list</li> <li>er:instances:listVpcAttachments</li> <li>er:instances:get</li> </ul> |
| POST /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/create   | cfw:instance:createTags        | -                                                                                                                                                                                                         |
| DELETE /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/delete | cfw:instance:deleteTags        | -                                                                                                                                                                                                         |
| PUT /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/save      | cfw:instance:saveTags          | -                                                                                                                                                                                                         |
| GET /v2/{project_id}/cfw-cfw/tags                            | cfw:instance:listProjectTags   | -                                                                                                                                                                                                         |
| GET /v1/{project_id}/capture-task                            | cfw:instance:listCaptureTask   | -                                                                                                                                                                                                         |
| POST /v1/{project_id}/capture-task                           | cfw:instance:createCaptureTask | -                                                                                                                                                                                                         |
| POST /v1/{project_id}/capture-task/stop                      | cfw:instance:stopCaptureTask   | -                                                                                                                                                                                                         |

| API                                                 | Action                               | Dependencies                                                                                                                                                                                                                |
|-----------------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/{project_id}/capture-task/batch-delete     | cfw:instance:deleteCaptureTask       | -                                                                                                                                                                                                                           |
| GET /v1/{project_id}/capture-task/capture-result    | cfw:instance:getCaptureTaskResult    | -                                                                                                                                                                                                                           |
| GET /v1/{project_id}/dns/servers                    | cfw:instance:listDomainParseServers  | -                                                                                                                                                                                                                           |
| PUT /v1/{project_id}/dns/servers                    | cfw:instance:updateDomainParseServer | -                                                                                                                                                                                                                           |
| PUT /v1/{project_id}/domain-set/{set_id}            | cfw:domainGroup:update               | -                                                                                                                                                                                                                           |
| DELETE /v1/{project_id}/domain-set/{set_id}         | cfw:domainGroup:delete               | -                                                                                                                                                                                                                           |
| GET /v1/{project_id}/domain-sets                    | cfw:domainGroup:list                 | -                                                                                                                                                                                                                           |
| POST /v1/{project_id}/system/multi-account/enable   | cfw:instance:enableMultiAccount      | <ul style="list-style-type: none"> <li>• organizations:trustedServices:list</li> <li>• organizations:organizations:get</li> <li>• organizations:trustedServices:enable</li> </ul>                                           |
| GET /v1/{project_id}/system/multi-account/accounts  | cfw:instance:listAccounts            | <ul style="list-style-type: none"> <li>• organizations:trustedServices:list</li> <li>• organizations:organizations:get</li> <li>• organizations:delegatedAdministrators:list</li> </ul>                                     |
| POST /v1/{project_id}/system/multi-account/accounts | cfw:instance:addAccount              | <ul style="list-style-type: none"> <li>• organizations:trustedServices:list</li> <li>• organizations:organizations:get</li> <li>• organizations:delegatedAdministrators:list</li> <li>• organizations:roots:list</li> </ul> |

| API                                                         | Action                            | Dependencies                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1/{project_id}/system/multi-account/organization-tree | cfw:instance:listOrganizationTree | <ul style="list-style-type: none"> <li>organizations:trustedServices:list</li> <li>organizations:organizations:get</li> <li>organizations:delegatedAdministrators:list</li> <li>organizations:roots:list</li> <li>organizations:ous:list</li> <li>organizations:accounts:list</li> </ul> |
| GET /v1/{project_id}/anti-virus/rule                        | cfw:instance:getAntiVirusRule     | -                                                                                                                                                                                                                                                                                        |
| PUT /v1/{project_id}/anti-virus/rule                        | cfw:instance:updateAntiVirusRule  | -                                                                                                                                                                                                                                                                                        |
| PUT /v1/{project_id}/report-profile/{report_profile_id}     | cfw:instance:updateReportProfile  | -                                                                                                                                                                                                                                                                                        |
| DELETE /v1/{project_id}/report-profile/{report_profile_id}  | cfw:instance:deleteReportProfile  | -                                                                                                                                                                                                                                                                                        |
| POST /v1/{project_id}/report-profile                        | cfw:instance:createReportProfile  | -                                                                                                                                                                                                                                                                                        |
| DELETE /v1/{project_id}/address-items                       | cfw:ipGroup:deleteIpGroupMember   | -                                                                                                                                                                                                                                                                                        |
| GET /v1/{project_id}/address-sets/{set_id}                  | cfw:ipGroup:getIpGroup            | -                                                                                                                                                                                                                                                                                        |
| GET /v1/{project_id}/address-items                          | cfw:ipGroup:listIpGroupMember     | -                                                                                                                                                                                                                                                                                        |
| GET /v1/{project_id}/address-sets                           | cfw:ipGroup:listIpGroups          | -                                                                                                                                                                                                                                                                                        |

| API                                                 | Action                                    | Dependencies |
|-----------------------------------------------------|-------------------------------------------|--------------|
| DELETE /v1/{project_id}/domain-set/domains/{set_id} | cfw:domainGroup:delete                    | -            |
| GET /v1/{project_id}/service-items                  | cfw:serviceGroup:listServiceGroupMember   | -            |
| DELETE /v1/{project_id}/service-items/{item_id}     | cfw:serviceGroup:deleteServiceGroupMember | -            |
| POST /v1/{project_id}/black-white-list              | cfw:blackWhiteList:create                 | -            |
| DELETE /v1/{project_id}/service-sets/{set_id}       | cfw:serviceGroup:delete                   | -            |
| POST /v1/{project_id}/firewalls/list                | cfw:instance:listInstance                 | -            |
| PUT /v1/{project_id}/service-sets/{set_id}          | cfw:serviceGroup:update                   | -            |
| POST /v1/{project_id}/eip/protect                   | cfw:eip:updateProtectStatus               | -            |
| POST /v1/{project_id}/domain-set                    | cfw:domainGroup:create                    | -            |
| GET /v1/{project_id}/firewall/exist                 | cfw:instance:getInstance                  | -            |
| DELETE /v1/{project_id}/acl-rule                    | cfw:acl:deleteAclRule                     | -            |
| GET /v1/{project_id}/domain/parse/{domain_name}     | cfw:instance:listDomainParseServers       | -            |
| POST /v1/{project_id}/acl-rule/count                | cfw:acl:listAclRules                      | -            |

| API                                               | Action                                    | Dependencies |
|---------------------------------------------------|-------------------------------------------|--------------|
| DELETE /v1/{project_id}/address-sets/{set_id}     | cfw:ipGroup:deleteIpGroup                 | -            |
| POST /v1/{project_id}/domain-set/domains/{set_id} | cfw:domainGroup:create                    | -            |
| GET /v1/{project_id}/service-sets                 | cfw:serviceGroup:list                     | -            |
| GET /v2/{project_id}/cfw-acl/tags                 | cfw:acl:listAclTags                       | -            |
| POST /v1/{project_id}/service-set                 | cfw:serviceGroup:create                   | -            |
| DELETE /v1/{project_id}/service-items             | cfw:serviceGroup:deleteServiceGroupMember | -            |
| POST /v1/{project_id}/ips/switch                  | cfw:instance:updateIpsStatus              | -            |
| POST /v1/{project_id}/ips/protect                 | cfw:instance:updateIpsMode                | -            |
| GET /v1/{project_id}/service-sets/{set_id}        | cfw:serviceGroup:get                      | -            |
| DELETE /v1/{project_id}/acl-rule/count            | cfw:acl:deleteHitCount                    | -            |
| PUT /v1/{project_id}/address-sets/{set_id}        | cfw:ipGroup:updateIpGroup                 | -            |
| DELETE /v1/{project_id}/acl-rule/{acl_rule_id}    | cfw:acl:deleteAclRule                     | -            |
| PUT /v1/{project_id}/acl-rule/action              | cfw:acl:updateAclRuleAction               | -            |

| API                                                     | Action                          | Dependencies |
|---------------------------------------------------------|---------------------------------|--------------|
| POST /v1/{project_id}/address-set                       | cfw:ipGroup:createIpGroup       | -            |
| PUT /v1/{project_id}/black-white-list/{list_id}         | cfw:blackWhiteList:update       | -            |
| DELETE /v1/{project_id}/address-items/{item_id}         | cfw:ipGroup:deleteIpGroupMember | -            |
| GET /v1/{project_id}/ips/switch                         | cfw:instance:getIpsStatus       | -            |
| PUT /v1/{project_id}/acl-rule/{acl_rule_id}             | cfw:acl:updateAclRule           | -            |
| GET /v1/{project_id}/vpcs/protection                    | cfw:instance:listProtectedVpc   | -            |
| GET /v1/{project_id}/eip-count/{object_id}              | cfw:eip:count                   | -            |
| GET /v1/{project_id}/black-white-lists                  | cfw:blackWhiteList:list         | -            |
| GET /v1/{project_id}/eips/protect                       | cfw:eip:list                    | -            |
| DELETE /v1/{project_id}/black-white-list/{list_id}      | cfw:blackWhiteList:delete       | -            |
| GET /v1/{project_id}/acl-rules                          | cfw:acl:listAclRules            | -            |
| GET /v1/{project_id}/domain-set/domains/{domain_set_id} | cfw:domainGroup:list            | -            |
| POST /v1/{project_id}/acl-rule                          | cfw:acl:createAclRule           | -            |

| API                                               | Action                                    | Dependencies |
|---------------------------------------------------|-------------------------------------------|--------------|
| PUT /v1/{project_id}/acl-rule/order/{acl_rule_id} | cfw:acl:setPriority                       | -            |
| POST /v1/{project_id}/address-items               | cfw:ipGroup:createIpGroupMember           | -            |
| GET /v1/{project_id}/ips/protect                  | cfw:instance:getIpsMode                   | -            |
| POST /v1/{project_id}/service-items               | cfw:serviceGroup:createServiceGroupMember | -            |
| GET /v1/{project_id}/cfw/logs/configuration       | cfw:instance:getLogConfig                 | -            |
| POST /v1/{project_id}/cfw/logs/configuration      | cfw:instance:updateLogConfig              | -            |
| POST /v2/{project_id}/firewall                    | cfw:instance:createInstance               | -            |
| GET /v3/{project_id}/jobs/{job_id}                | cfw:instance:listInstance                 | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-150](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CFW.

**Table 3-150** Resource types supported by CFW

| Resource Type  | URN                                                          |
|----------------|--------------------------------------------------------------|
| blackWhiteList | cfw:<region>:<account-id>:blackWhiteList:<blackWhiteList-id> |



| Resource Type | URN                                                      |
|---------------|----------------------------------------------------------|
| acl           | cfw:<region>:<account-id>:acl:<acl-id>                   |
| instance      | cfw:<region>:<account-id>:instance:<fwInstance-id>       |
| serviceGroup  | cfw:<region>:<account-id>:serviceGroup:<serviceGroup-id> |
| domainGroup   | cfw:<region>:<account-id>:domainGroup:<domainGroup-id>   |
| ipGroup       | cfw:<region>:<account-id>:ipGroup:<ipGroup-id>           |
| eip           | cfw:<region>:<account-id>:eip:<eip-id>                   |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, cfw) apply only to operations of the xx service. For details, see [Table 3-151](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by CFW

The following table lists the condition keys that you can define in identity policies for CFW. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-151** Service-specific condition keys supported by CFW

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                  |
|--------------------------------|--------|-------------------------------|--------------------------------------------------------------|
| cfw:LogGroupId                 | string | Single-valued                 | Filters access based on the LTS log group ID in the request. |

### 3.7.4 Cloud Bastion Host (CBH)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.

- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CBH, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CBH, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CBH.

**Table 3-152** Actions supported by CBH

| Action                  | Description                                               | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| cbh::listAvailableZones | Grants permission to list AZs.                            | List         | -                           | -             | -     |
| cbh::getEcsQuota        | Grants permission to query ECS resource quotas.           | Read         | -                           | -             | -     |
| cbh::getQuota           | Grants permission to query the quota of the bastion host. | Read         | -                           | -             | -     |
| cbh::listSpecifications | Grants permission to list bastion host specifications.    | List         | -                           | -             | -     |

| Action                         | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                              | Alias |
|--------------------------------|-------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cbh:instance:listInstances     | Grants permission to list bastion hosts.        | List         | instance *                  | -                                                                                                                                          | -     |
| cbh:instance:getInstanceStatus | Grants permission to query bastion host status. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:startInstance     | Grants permission to start bastion host.        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:stopInstance      | Grants permission to stop bastion host.         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:rebootInstance    | Grants permission to reboot bastion host.       | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:upgradeInstance   | Grants permission to upgrade bastion host.      | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |

| Action                                | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                              | Alias |
|---------------------------------------|------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cbh:instance:loginInstance            | Grants permission to login bastion host as the IAM user.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:resetInstancePassword    | Grants permission to reset the password of bastion host.   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:resetInstanceLoginMethod | Grants permission to reset the login mode of bastion host. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:deleteInstance           | Grants permission to delete faulty bastion host.           | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:alterInstance            | Grants permission to alter bastion host.                   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:createInstance           | Grants permission to create bastion host.                  | Write        | instance *                  | -                                                                                                                                          | -     |

| Action                                   | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                | Alias |
|------------------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                          |                                                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/tag-key</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">cbh:VpcId</a></li> <li>• <a href="#">cbh:SubnetId</a></li> <li>• <a href="#">cbh:AllowBindPublicIp</a></li> </ul> |       |
| cbh:instance:bindInstanceEip             | Grants permission to bind an EIP to bastion host.                                      | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul>                                                                                                                                                                   | -     |
| cbh:instance:unbindInstanceEip           | Grants permission to unbind an EIP to bastion host.                                    | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul>                                                                                                                                                                   | -     |
| cbh:instance:updateInstanceSecurityGroup | Grants permission to update the security group of bastion host.                        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul>                                                                                                                                                                   | -     |
| cbh::operateAuthorization                | Grants permission to create or cancel the authorization of cloud bastion host service. | Write        | -                           | -                                                                                                                                                                                                                                                                                                            | -     |

| Action                           | Description                                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                              | Alias |
|----------------------------------|---------------------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------|
| cbh::getAuthorization            | Grants permission to query the authorization of cloud bastion host service from the tenant. | Read         | -                           | -                                                                                                                                          | -     |
| cbh::listTags                    | Grants permission to list all tags.                                                         | List         | -                           | -                                                                                                                                          | -     |
| cbh:instance:getInstanceTags     | Grants permission to query the tag information of bastion host instance.                    | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
| cbh:instance:countInstancesByTag | Grants permission to count the number of instances that meet the label criteria.            | List         | instance *                  | -                                                                                                                                          | -     |
| cbh:instance:listInstancesByTag  | Grants permission to filter instances by tags.                                              | List         | -                           | -                                                                                                                                          | -     |
| cbh:instance:operateInstanceTags | Grants permission to operate resource tags of bastion host instance.                        | Tagging      | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/tag-key</a></li> </ul> | -     |
|                                  |                                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/tag-key</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |       |

| Action                        | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|-------------------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| cbh:instance:getOmUrl         | Grants permission to get O&M url.           | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | cbh:instance:getOmUrl |
| cbh:instance:rollbackInstance | Grants permission to rollback bastion host. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | cbh:instance:upgrade  |

Each API of CBH usually supports one or more actions. [Table 3-153](#) lists the supported actions and dependencies.

**Table 3-153** Actions and dependencies supported by CBH APIs

| API                                             | Action                       | Dependencies                |
|-------------------------------------------------|------------------------------|-----------------------------|
| GET /v2/{project_id}/cbs/available-zone         | cbh::listAvailableZones      | -                           |
| GET /v2/{project_id}/cbs/instance/specification | cbh::listSpecifications      | -                           |
| GET /v2/{project_id}/cbs/instance/list          | cbh:instance:listInstances   | eps:enterpriseProjects:list |
| POST /v2/{project_id}/cbs/instance/start        | cbh:instance:startInstance   | -                           |
| POST /v2/{project_id}/cbs/instance/stop         | cbh:instance:stopInstance    | -                           |
| POST /v2/{project_id}/cbs/instance/upgrade      | cbh:instance:upgradeInstance | -                           |



| API                                                           | Action                                   | Dependencies                                                                                                                                                                              |
|---------------------------------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/cbs/instance/login                      | cbh:instance:loginInstance               | -                                                                                                                                                                                         |
| PUT /v2/{project_id}/cbs/instance/password                    | cbh:instance:resetInstancePassword       | -                                                                                                                                                                                         |
| PUT /v2/{project_id}/cbs/instance/login-method                | cbh:instance:resetInstanceLoginMethod    | -                                                                                                                                                                                         |
| DELETE /v2/{project_id}/cbs/instance                          | cbh:instance:deleteInstance              | -                                                                                                                                                                                         |
| POST /v2/{project_id}/cbs/instance                            | cbh:instance:createInstance              | <ul style="list-style-type: none"> <li>vpc:quotas:list</li> <li>vpc:subnets:list</li> <li>vpc:subnets:get</li> <li>vpc:securityGroups:list</li> <li>ecs:cloudServerFlavors:get</li> </ul> |
| PUT /v2/{project_id}/cbs/instance/{server_id}/security-groups | cbh:instance:updateInstanceSecurityGroup | vpc:ports:update                                                                                                                                                                          |
| GET /v2/{project_id}/cbs/agency/authorization                 | cbh::getAuthorization                    | -                                                                                                                                                                                         |
| GET /v2/{project_id}/cbs/instance/tags                        | cbh::listTags                            | -                                                                                                                                                                                         |
| GET /v2/{project_id}/cbs/instance/{resource_id}/tags          | cbh:instance:getInstanceTags             | -                                                                                                                                                                                         |
| POST /v2/{project_id}/cbs/instance/count                      | cbh:instance:countInstancesByTag         | -                                                                                                                                                                                         |
| POST /v2/{project_id}/cbs/instance/filter                     | cbh:instance:listInstancesByTag          | -                                                                                                                                                                                         |

| API                                                          | Action                           | Dependencies                                                                                       |
|--------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/cbs/instance/{server_id}/eip/bind      | cbh:instance:bindInstanceEip     | <ul style="list-style-type: none"> <li>eip:publicIps:list</li> <li>eip:publicIps:update</li> </ul> |
| POST /v2/{project_id}/cbs/instance/{server_id}/eip/unbind    | cbh:instance:unbindInstanceEip   | <ul style="list-style-type: none"> <li>eip:publicIps:update</li> <li>eip:publicIps:list</li> </ul> |
| GET /v2/{project_id}/cbs/instance/ecs-quota                  | cbh::getEcsQuota                 | ecs:cloudServerFlavors:get                                                                         |
| GET /v2/{project_id}/cbs/instance/quota                      | cbh::getQuota                    | -                                                                                                  |
| GET /v2/{project_id}/cbs/instance/{server_id}/status         | cbh:instance:getInstanceStatus   | -                                                                                                  |
| POST /v2/{project_id}/cbs/instance/reboot                    | cbh:instance:rebootInstance      | -                                                                                                  |
| PUT /v2/{project_id}/cbs/instance                            | cbh:instance:alterInstance       | -                                                                                                  |
| POST /v2/{project_id}/cbs/agency/authorization               | cbh::operateAuthorization        | -                                                                                                  |
| POST /v2/{project_id}/cbs/instance/{resource_id}/tags/action | cbh:instance:operateInstanceTags | -                                                                                                  |
| GET /v2/{project_id}/cbs/instance/get-om-url                 | cbh:instance:getOmUrl            | -                                                                                                  |
| POST /v2/{project_id}/cbs/instance/rollback                  | cbh:instance:rollbackInstance    | -                                                                                                  |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-154](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CBH.

**Table 3-154** Resource types supported by CBH

| Resource Type | URN                                              |
|---------------|--------------------------------------------------|
| instance      | cbh:<region>:<account-id>:instance:<instance-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, cbh) apply only to operations of the xx service. For details, see [Table 3-155](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by CBH

The following table lists the condition keys that you can define in identity policies for CBH. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-155** Service-specific condition keys supported by CBH

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                  |
|--------------------------------|---------|-------------------------------|------------------------------------------------------------------------------|
| cbh:VpcId                      | string  | Single-valued                 | Filters access to control which VPC (ID) the instance can communicate with.  |
| cbh:SubnetId                   | string  | Single-valued                 | Filters access to control which CIDR (ID) the instance can communicate with. |
| cbh:AllowBindPublicIp          | boolean | Single-valued                 | Filters access to control whether EIPs can be bound to the instance.         |

### 3.7.5 Cloud Certificate & Manager (CCM)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN for the Resource element in your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table.

For details about the resource types defined by the PCA, see [Table 3-158](#).

- The **Condition Key** contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key only takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by PCA, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for PCA.

**Table 3-156** Actions supported by PCA

| Action        | Description                                   | Access Level | Resource Type (*: Required) | Condition Key            | Alias |
|---------------|-----------------------------------------------|--------------|-----------------------------|--------------------------|-------|
| pca:ca:create | Grants the permission to create a private CA. | write        | ca *                        | -                        | -     |
|               |                                               |              | -                           | g:EnterpriseProjectId    |       |
| pca:ca:delete | Grants the permission to delete a private CA. | write        | ca *                        | g:ResourceTag /<tag-key> | -     |
|               |                                               |              | -                           | g:EnterpriseProjectId    |       |

| Action          | Description                                                                            | Access Level | Resource Type (*: Required) | Condition Key            | Alias         |
|-----------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------|---------------|
| pca:ca:disable  | Grants the permission to disable a private CA.                                         | write        | ca *                        | g:ResourceTag /<tag-key> | -             |
|                 |                                                                                        |              | -                           | g:EnterpriseProjectId    |               |
| pca:ca:enable   | Grants the permission to enable a private CA.                                          | write        | ca *                        | g:ResourceTag /<tag-key> | -             |
|                 |                                                                                        |              | -                           | g:EnterpriseProjectId    |               |
| pca:ca:export   | Grants the permission to export a private CA certificate.                              | read         | ca *                        | g:ResourceTag /<tag-key> | -             |
|                 |                                                                                        |              | -                           | g:EnterpriseProjectId    |               |
| pca:ca:getCsr   | Grants the permission to export the certificate signing request (CSR) of a private CA. | read         | ca *                        | g:ResourceTag /<tag-key> | -             |
|                 |                                                                                        |              | -                           | g:EnterpriseProjectId    |               |
| pca:ca:import   | Grants the permission to import a certificate as a private CA certificate.             | write        | ca *                        | -                        | -             |
|                 |                                                                                        |              | -                           | g:EnterpriseProjectId    |               |
| pca:ca:activate | Grants the permission to activate a private CA.                                        | write        | ca *                        | g:ResourceTag /<tag-key> | pca:ca:active |
|                 |                                                                                        |              | -                           | g:EnterpriseProjectId    |               |
| pca:ca:list     | Grants the permission to query the private CA list.                                    | list         | ca *                        | -                        | -             |
|                 |                                                                                        |              | -                           | g:EnterpriseProjectId    |               |

| Action           | Description                                                      | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                    | Alias |
|------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------|
| pca:ca:restore   | Grants the permission to restore a private CA.                   | write        | ca *                        | g:ResourceTag /<tag-key>                                                                                                         | -     |
|                  |                                                                  |              | -                           | g:EnterpriseProjectId                                                                                                            |       |
| pca:ca:revoke    | Grants the permission to revoke a private CA.                    | write        | ca *                        | g:ResourceTag /<tag-key>                                                                                                         | -     |
|                  |                                                                  |              | -                           | g:EnterpriseProjectId                                                                                                            |       |
| pca:ca:get       | Grants the permission to query private CA details.               | read         | ca *                        | g:ResourceTag /<tag-key>                                                                                                         | -     |
|                  |                                                                  |              | -                           | g:EnterpriseProjectId                                                                                                            |       |
| pca:ca:quota     | Grants the permission to query the private CA quota.             | read         | -                           | -                                                                                                                                | -     |
| pca:ca:createTag | Grants the permission to create or update tags for a private CA. | tagging      | ca *                        | g:ResourceTag /<tag-key>                                                                                                         | -     |
|                  |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |       |
| pca:ca:deleteTag | Grants the permission to delete a private CA tag.                | tagging      | ca *                        | g:ResourceTag /<tag-key>                                                                                                         | -     |
|                  |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:TagKeys</li> </ul>                                       |       |
| pca:ca:listTags  | Grants the permission to query the tag list of a private CA.     | list         | ca *                        | g:ResourceTag /<tag-key>                                                                                                         | -     |
|                  |                                                                  |              | -                           | g:EnterpriseProjectId                                                                                                            |       |

| Action                | Description                                                        | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                    | Alias                      |
|-----------------------|--------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| pca:ca:listAllTags    | Grants the permission to query the private CA tag list.            | list         | ca *                        | -                                                                                                                                | -                          |
| pca:ca:listByTag      | Grants the permission to query the private CA list by tag.         | list         | ca *                        | -                                                                                                                                | -                          |
|                       |                                                                    |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |                            |
| pca:ca:issueCert      | Grants the permission to issue a private certificate.              | write        | ca *                        | -                                                                                                                                | -                          |
|                       |                                                                    |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>pca:CommonName</li> </ul>                                  |                            |
| pca:ca:issueCertByCsr | Grants the permission to issue private certificates based on CSRs. | write        | ca *                        | -                                                                                                                                | pca:ca:issueCertThroughCSR |
|                       |                                                                    |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>pca:CommonName</li> </ul>                                  |                            |
| pca:cert:delete       | Grants the permission to delete a private certificate.             | write        | -                           | g:EnterpriseProjectId                                                                                                            | -                          |
| pca:cert:export       | Grants the permission to export a private certificate.             | read         | -                           | g:EnterpriseProjectId                                                                                                            | -                          |
| pca:cert:list         | Grants the permission to query the private certificate list.       | list         | -                           | g:EnterpriseProjectId                                                                                                            | -                          |



| Action               | Description                                                           | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                    | Alias           |
|----------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------|
| pca:ca:revokeCert    | Grants the permission to revoke a private certificate.                | write        | ca *                        | g:ResourceTag/<tag-key>                                                                                                          | pca:cert:revoke |
|                      |                                                                       |              | -                           | g:EnterpriseProjectId                                                                                                            |                 |
| pca:cert:get         | Grants the permission to query private certificate details.           | read         | -                           | g:EnterpriseProjectId                                                                                                            | -               |
| pca:cert:quota       | Grants the permission to query the private certificate quota.         | read         | -                           | -                                                                                                                                | -               |
| pca:cert:createTag   | Grants the permission to create or update private certificate tags.   | tagging      | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> | -               |
| pca:cert:deleteTag   | Grants the permission to delete a private certificate tag.            | tagging      | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:TagKeys</li> </ul>                                       | -               |
| pca:cert:listTags    | Grants the permission to query the tag list of a private certificate. | list         | -                           | g:EnterpriseProjectId                                                                                                            | -               |
| pca:cert:listAllTags | Grants the permission to query the private certificate tag list.      | list         | -                           | -                                                                                                                                | -               |

| Action             | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                    | Alias |
|--------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------|
| pca:cert:listByTag | Grants the permission to query the private certificate list by tag. | list         | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> | -     |
| pca:ca:disableCrl  | Grants the permission to disable CRLs.                              | write        | ca *                        | g:ResourceTag/<tag-key>                                                                                                          | -     |
|                    |                                                                     |              | -                           | g:EnterpriseProjectId                                                                                                            |       |
| pca:ca:enableCrl   | Grants the permission to enable CRLs.                               | write        | ca *                        | g:ResourceTag/<tag-key>                                                                                                          | -     |
|                    |                                                                     |              | -                           | g:EnterpriseProjectId                                                                                                            |       |

Each API of PCA usually supports one or more actions. [Table 3-157](#) lists the actions and dependencies supported by PCA APIs.

**Table 3-157** Actions and dependencies supported by PCA APIs

| API                                                      | Action         | Dependencies |
|----------------------------------------------------------|----------------|--------------|
| POST /v1/private-certificate-authorities                 | pca:ca:create  | -            |
| POST /v1/private-certificate-authorities/order           | pca:ca:create  | -            |
| DELETE /v1/private-certificate-authorities/{ca_id}       | pca:ca:delete  | -            |
| POST /v1/private-certificate-authorities/{ca_id}/disable | pca:ca:disable | -            |

| API                                                          | Action           | Dependencies |
|--------------------------------------------------------------|------------------|--------------|
| POST /v1/private-certificate-authorities/{ca_id}/enable      | pca:ca:enable    | -            |
| POST /v1/private-certificate-authorities/{ca_id}/export      | pca:ca:export    | -            |
| GET /v1/private-certificate-authorities/{ca_id}/csr          | pca:ca:getCsr    | -            |
| POST /v1/private-certificate-authorities/{ca_id}/import      | pca:ca:import    | -            |
| POST /v1/private-certificate-authorities/{ca_id}/activate    | pca:ca:activate  | -            |
| GET /v1/private-certificate-authorities                      | pca:ca:list      | -            |
| POST /v1/private-certificate-authorities/{ca_id}/restore     | pca:ca:restore   | -            |
| POST /v1/private-certificate-authorities/{ca_id}/revoke      | pca:ca:revoke    | -            |
| GET /v1/private-certificate-authorities/{ca_id}              | pca:ca:get       | -            |
| GET /v1/private-certificate-authorities/quotas               | pca:ca:quota     | -            |
| POST /v1/private-certificate-authorities/{ca_id}/tags/create | pca:ca:createTag | -            |

| API                                                                | Action                | Dependencies |
|--------------------------------------------------------------------|-----------------------|--------------|
| DELETE /v1/private-certificate-authorities/{ca_id}/tags/delete     | pca:ca:deleteTag      | -            |
| POST /v1/private-certificate-authorities/{ca_id}/tags              | pca:ca:createTag      | -            |
| GET /v1/private-certificate-authorities/{ca_id}/tags               | pca:ca:listTags       | -            |
| GET /v1/private-certificate-authorities/tags                       | pca:ca:listAllTags    | -            |
| POST /v1/private-certificate-authorities/resource-instances/filter | pca:ca:listByTag      | -            |
| POST /v1/private-certificates                                      | pca:ca:issueCert      | -            |
| POST /v1/private-certificates/csr                                  | pca:ca:issueCertByCsr | -            |
| DELETE /v1/private-certificates/{certificate_id}                   | pca:cert:delete       | -            |
| POST /v1/private-certificates/{certificate_id}/export              | pca:cert:export       | -            |
| GET /v1/private-certificates                                       | pca:cert:list         | -            |
| POST /v1/private-certificates/{certificate_id}/revoke              | pca:ca:revokeCert     | -            |
| GET /v1/private-certificates/{certificate_id}                      | pca:cert:get          | -            |
| GET /v1/private-certificates/quotas                                | pca:cert:quota        | -            |

| API                                                          | Action               | Dependencies |
|--------------------------------------------------------------|----------------------|--------------|
| POST /v1/private-certificates/{certificate_id}/tags/create   | pca:cert:createTag   | -            |
| DELETE /v1/private-certificates/{certificate_id}/tags/delete | pca:cert:deleteTag   | -            |
| POST /v1/private-certificates/{certificate_id}/tags          | pca:cert:createTag   | -            |
| GET /v1/private-certificates/{certificate_id}/tags           | pca:cert:listTags    | -            |
| GET /v1/private-certificates/tags                            | pca:cert:listAllTags | -            |
| POST /v1/private-certificates/resource-instances/filter      | pca:cert:listByTag   | -            |
| POST /v1/private-certificate-authorities/{ca_id}/crl/disable | pca:ca:disableCrl    | -            |
| POST /v1/private-certificate-authorities/{ca_id}/crl/enable  | pca:ca:enableCrl     | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-158](#), the resource URN must be specified in the identity policy using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the **Resource** element is marked with an asterisk (\*) and the policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for PCA.

**Table 3-158** Resource types supported by PCA

| Resource Type | URN                                  |
|---------------|--------------------------------------|
| ca            | pca:<region>:<account-id>:ca:<ca-id> |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, IAM automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **pca:**) apply only to operations of the corresponding service. For details, see [Table 3-159](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, a condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

The following table lists the condition keys that you can define in identity policies for PCA. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-159** Service-specific condition keys supported by PCA

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                           |
|--------------------------------|--------|-------------------------------|---------------------------------------------------------------------------------------|
| pca:CommonName                 | string | Single-valued                 | Filters access based on the common name of the certificate in the request parameters. |

### 3.7.6 Database Security Service (DBSS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

#### Action

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN for the **Resource** element of your statements.
  - Required resources are marked with asterisks (\*) in the table.

For details about the resource types defined by DBSS, see [Resource](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DBSS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for identity policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DBSS.

**Table 3-160** Actions supported by DBSS

| Action                                 | Description                                                    | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|----------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:listSqlInjectRules  | Grants permission to query SQL injection rules.                | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:listSqls            | Grants permission to obtain audit results.                     | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:switchSqlInjectRule | Grants permission to enable or disable SQL injection policies. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:addSqlInjectRule    | Grants permission to add custom SQL injection rules.           | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:orderSqlInjectRule  | Grants permission to sort SQL rules by priority.               | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |



| Action                                 | Description                                                    | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|----------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:createReporter      | Grants permission to generate reports immediately.             | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:listReporters       | Grants permission to query report information.                 | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:getRiskRuleDetail   | Grants permission to query a specified risk rule policy.       | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:listAlarmEmails     | Grants permission to query alarm email information.            | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:downloadReporter    | Grants permission to download reports.                         | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:listAuditScopeRules | Grants permission to query the policy list for an audit scope. | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |

| Action                               | Description                                                       | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|--------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:addSensitiveRule  | Grants permission to add a privacy data protection rule.          | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:editSensitiveRule | Grants permission to edit privacy data protection rules.          | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:deleteReporter    | Grants permission to delete reports.                              | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:listOperationLog  | Grants permission to query user operation logs.                   | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:listMonitorInfos  | Grants permission to query audit instance monitoring information. | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:listSessionInfo   | Grants permission to query audit instance session information.    | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |

| Action                           | Description                                                       | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|----------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:switchBackup  | Grants permission to enable or disable the backup function.       | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss::downloadLicense            | Grants permission to download a sales license.                    | Read         | -                           | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss::deleteAuditInstanceJob     | Grants permission to delete failed audit instance creation tasks. | Write        | -                           | -                                                                                                                                                  | dbss:auditInstance:delete        |
| dbss::listRdsDb                  | Grants permission to query RDS databases.                         | List         | -                           | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss:auditInstance:instanceStart | Grants permission to enable audit instances.                      | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:start         |
| dbss:auditInstance:reboot        | Grants permission to restart audit instances.                     | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                |
| dbss:auditInstance:stop          | Grants permission to disable audit instances.                     | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                |

| Action                                 | Description                                                          | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|----------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:upgrade             | Grants permission to upgrade audit instances.                        | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss::queryUpgradeStatus               | Grants permission to query the upgrade status of an audit instance.  | List         | -                           | -                                                                                                                                                  | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:updateSecurityGroup | Grants permission to modify the security group of an audit instance. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:modifyAttribute     | Grants permission to modify attributes of audit instances.           | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:downloadAgent       | Grants permission to download agents.                                | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:switchAgent         | Grants permission to enable or disable agents.                       | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |

| Action                              | Description                                             | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|-------------------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:listAgents       | Grants permissions to obtain the agent list.            | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:deleteAgent      | Grants permissions to delete agents.                    | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:addAgent         | Grants permissions to add agents.                       | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:previewReporter  | Grants permissions to preview reports.                  | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:setAlarmConfig   | Grants permission to configure alarm information.       | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:configAlarmEmail | Grants permission to configure alarm email information. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |

| Action                                           | Description                                                                 | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                         | Alias                            |
|--------------------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:getAlarmConfig                | Grants permission to query alarm configurations.                            | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                    | dbss:auditInstance:list          |
| dbss:auditInstance:listRiskRules                 | Grants permission to query risk rule policies.                              | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                    | dbss:auditInstance:list          |
| dbss:auditInstance:exportInstancesDatabaseConfig | Grants permission to export database configurations.                        | List         | auditInstance *             | -                                                                                                                                                                                                                                                                     | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:createOnPeriod                | Grants permission to create audit instances in yearly/monthly billing mode. | Write        | auditInstance *             | -                                                                                                                                                                                                                                                                     | dbss:auditInstance:createOnOrder |
|                                                  |                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">dbss:VpcId</a></li> <li>• <a href="#">dbss:SubnetId</a></li> </ul> |                                  |
| dbss:auditInstance:editSqlInjectRule             | Grants permission to edit custom SQL injection rules.                       | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                    | dbss:auditInstance:createOnOrder |

| Action                                  | Description                                                | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|-----------------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:deleteSqlInjectRule  | Grants permission to delete custom SQL injection rules.    | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:deleteSensitiveRule  | Grants permission to delete privacy data protection rules. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:deleteAuditScopeRule | Grants permission to delete an audit scope rule.           | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:deleteRiskRule       | Grants permission to delete a risk rule.                   | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:deleteBackup         | Grants permission to delete local backup information.      | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:listBackups          | Grants permission to query backup information.             | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |

| Action                                | Description                                                      | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                         | Alias                            |
|---------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:getBackupConfig    | Grants permission to obtain backup configuration information.    | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                    | dbss:auditInstance:list          |
| dbss:auditInstance:editAuditScopeRule | Grants permission to edit an audit scope rule.                   | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                    | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:instanceList       | Grants permission to query audit instance information.           | List         | auditInstance *             | -                                                                                                                                                                                                                                                                     | dbss:auditInstance:list          |
| dbss:auditInstance:createOnDemand     | Grants permission to create audit instances in pay-per-use mode. | Write        | auditInstance *             | -                                                                                                                                                                                                                                                                     | -                                |
|                                       |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">dbss:VpcId</a></li> <li>• <a href="#">dbss:SubnetId</a></li> </ul> |                                  |
| dbss::listCommonInfo                  | Grants permission to query public information.                   | List         | -                           | -                                                                                                                                                                                                                                                                     | dbss:auditInstance:list          |



| Action                                      | Description                                                                          | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|---------------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:listInstancesSummaryInfo | Grants permission to query the overview of all audit instances.                      | List         | auditInstance *             | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss::getAuditInstancesSummaryTaskStatus    | Grants permission to query the status of overview tasks.                             | Read         | -                           | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss::updateAuditInstancesSummaryInfo       | Grants permission to update the overview of all audit instances.                     | Write        | -                           | -                                                                                                                                                  | dbss:auditInstance:start         |
| dbss:auditInstance:setReporterConfig        | Grants permission to modify the scheduled task configuration information of reports. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:getReporterConfig        | Grants permission to obtain the scheduled task configuration information of reports. | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:addBareDatabase          | Grants permission to add a self-built database.                                      | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |

| Action                                  | Description                                               | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|-----------------------------------------|-----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:listDatabases        | Grants permission to query the database list.             | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:switchDatabase       | Grants permission to enable or disable database audit.    | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:deleteDatabase       | Grants permission to delete a database.                   | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:addAuditScopeRule    | Grants permission to add an audit scope rule.             | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:switchAuditScopeRule | Grants permission to enable or disable audit scope rules. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:addRiskRule          | Grants permission to add a risk rule.                     | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |

| Action                                                 | Description                                                    | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|--------------------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:switchRiskRule                      | Grants permission to enable or disable a risk rule.            | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:editRiskRule                        | Grants permission to edit risk rules.                          | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:setRiskRulePriority                 | Grants permission to set risk rule priorities.                 | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:listStatistics                      | Grants permission to query the overview of audit instances.    | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:listSensitiveRules                  | Grants permission to query privacy data masking rules.         | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:modifySensitiveRuleSaveResultSwitch | Grants permission to enable or disable the result set storage. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |

| Action                                                | Description                                                               | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|-------------------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:modifySensitiveRuleAnonymizeSwitch | Grants permission to enable or disable the privacy data masking function. | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:switchSensitiveRule                | Grants permission to enable or disable privacy data protection rules.     | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:listAlarmItems                     | Grants permission to query alarm information.                             | List         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:markAlarm                          | Grants permission to mark alarms.                                         | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:deleteAlarm                        | Grants permission to delete alarms.                                       | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:restoreBackup                      | Grants permission to restore backups.                                     | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |

| Action                                     | Description                                             | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|--------------------------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss:auditInstance:retryBackup             | Grants permissions to retry backups.                    | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:getRiskBackupConfigInfo | Grants permission to obtain risk export configurations. | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:switchRiskBackup        | Grants permission to enable or disable risk export.     | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:getRiskBackupBucketInfo | Grants permission to obtain OBS bucket for risk export. | Read         | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:list          |
| dbss:auditInstance:setRiskBackupBucketInfo | Grants permission to set OBS bucket for risk export.    | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |
| dbss:auditInstance:addRdsDatabase          | Grants permission to add an RDS database.               | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:createOnOrder |

| Action                            | Description                                                                    | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                      | Alias                            |
|-----------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| dbss::getServerInfo               | Grants permission to obtain DBSS information.                                  | Read         | -                           | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss::getAuditInstanceJob         | Grants permission to view the creation information about audit instance tasks. | Read         | -                           | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss:auditInstance:listJobs       | Grants permission to list the creation information about audit instance tasks. | List         | auditInstance *             | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss::listObsBuckets              | Grants permission to query the OBS bucket list.                                | List         | -                           | -                                                                                                                                                  | dbss:auditInstance:list          |
| dbss:auditInstance:instanceDelete | Grants permission to delete audit instances.                                   | Write        | auditInstance *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dbss:auditInstance:delete        |
| dbss::listResourcesByTag          | Grants permission to query audit instances by tag.                             | List         | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              | dbss:auditInstance:list          |
| dbss::tagResource                 | Grants permission to add instance tags in batches.                             | Tagging      | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              | dbss:auditInstance:createOnOrder |

| Action                    | Description                                           | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                         | Alias                     |
|---------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| dbss::unTagResource       | Grants permission to delete instance tags in batches. | Tagging      | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | dbss:auditInstance:delete |
| dbss::listTags            | Grants permission to query all tags of a project.     | List         | -                           | -                                                                                                                                     | dbss:auditInstance:list   |
| dbss::listTagsForResource | Grants permission to query instance tags.             | List         | -                           | -                                                                                                                                     | dbss:auditInstance:list   |

Each API of DBSS usually supports one or more actions. [Table 3-161](#) lists the supported actions and dependencies.

**Table 3-161** Actions and dependencies supported by DBSS APIs

| API                                                                     | Action                                   | Dependency |
|-------------------------------------------------------------------------|------------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rules           | dbss:auditInstance:listSqlInjectionRules | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/list-rules      | dbss:auditInstance:listSqlInjectionRules | -          |
| POST /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/sql-injections | dbss:auditInstance:listSqlInjectionRules | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sqls                     | dbss:auditInstance:listSqls              | -          |

| API                                                                          | Action                                 | Dependency |
|------------------------------------------------------------------------------|----------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/sqls/list-sqls                | dbss:auditInstance:listSqls            | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rule/switch          | dbss:auditInstance:switchSqlInjectRule | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/switch               | dbss:auditInstance:switchSqlInjectRule | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rule                 | dbss:auditInstance:addSqlInjectRule    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql                      | dbss:auditInstance:addSqlInjectRule    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rules/rank           | dbss:auditInstance:orderSqlInjectRule  | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/rank-sql             | dbss:auditInstance:orderSqlInjectRule  | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/reports                       | dbss:auditInstance:createReporter      | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/reports/results/create-report | dbss:auditInstance:createReporter      | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/reports/list                  | dbss:auditInstance:listReporters       | -          |



| API                                                                                       | Action                                 | Dependency |
|-------------------------------------------------------------------------------------------|----------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/reports/list-reports                       | dbss:auditInstance:listReporters       | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/{risk_id}                         | dbss:auditInstance:getRiskRuleDetail   | -          |
| GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/risk/{risk_id}                    | dbss:auditInstance:getRiskRuleDetail   | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/operation/emails                            | dbss:auditInstance:listAlarmEmails     | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/operation/list-emails                       | dbss:auditInstance:listAlarmEmails     | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}                         | dbss:auditInstance:downloadReporter    | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/results/{report_id}/download-report | dbss:auditInstance:downloadReporter    | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes                                 | dbss:auditInstance:listAuditScopeRules | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/list-scope                       | dbss:auditInstance:listAuditScopeRules | -          |

| API                                                                               | Action                                 | Dependency |
|-----------------------------------------------------------------------------------|----------------------------------------|------------|
| GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/scopes                    | dbss:auditInstance:listAuditScopeRules | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/masks                     | dbss:auditInstance:listSensitiveRules  | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/list-rules           | dbss:auditInstance:listSensitiveRules  | -          |
| GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/sensitive/masks                | dbss:auditInstance:listSensitiveRules  | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/masks                    | dbss:auditInstance:addSensitiveRule    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/add-rule            | dbss:auditInstance:addSensitiveRule    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/masks/{rule_id}          | dbss:auditInstance:editSensitiveRule   | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/{rule_id}/edit-rule | dbss:auditInstance:editSensitiveRule   | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/templates                   | dbss:auditInstance:listReporters       | -          |

| API                                                                                        | Action                              | Dependency |
|--------------------------------------------------------------------------------------------|-------------------------------------|------------|
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/list-templates                       | dbss:auditInstance:listReporters    | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/rule/risk                                    | dbss:auditInstance:listRiskRules    | -          |
| GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/rule/risk                               | dbss:auditInstance:listRiskRules    | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}                       | dbss:auditInstance:deleteReporter   | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/reports/results/{report_id}/delete-report | dbss:auditInstance:deleteReporter   | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/operate-log                         | dbss:auditInstance:listOperateLog   | -          |
| POST /dbss/v1/{project_id}/{instance_id}/dbss/audit/operate-log                            | dbss:auditInstance:listOperateLog   | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/monitorinfo                       | dbss:auditInstance:listMonitorInfos | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/get-monitorinfo                   | dbss:auditInstance:listMonitorInfos | -          |

| API                                                                                  | Action                             | Dependency                         |
|--------------------------------------------------------------------------------------|------------------------------------|------------------------------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/clientsession       | dbss:auditInstance:listSessionInfo | -                                  |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/list-clientsession  | dbss:auditInstance:listSessionInfo | -                                  |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/accountsession      | dbss:auditInstance:listSessionInfo | -                                  |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sessionstatistics/list-accountsession | dbss:auditInstance:listSessionInfo | -                                  |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/stop                           | dbss:auditInstance:switchBackup    | dbss:auditInstance:getBackupConfig |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/stop-backup                    | dbss:auditInstance:switchBackup    | dbss:auditInstance:getBackupConfig |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/start                          | dbss:auditInstance:switchBackup    | dbss:auditInstance:getBackupConfig |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/start-backup                   | dbss:auditInstance:switchBackup    | dbss:auditInstance:getBackupConfig |
| GET /dbss/v1/{project_id}/dbss/saleslicense/download                                 | dbss::downloadLicense              | -                                  |

| API                                                            | Action                            | Dependency |
|----------------------------------------------------------------|-----------------------------------|------------|
| GET /dbss/v1/{project_id}/dbss/download-saleslicense           | dbss::downloadLicense             | -          |
| DELETE /dbss/v1/{project_id}/dbss/audit/job/{failed_id}        | dbss::deleteAuditInstance-Job     | -          |
| DELETE /dbss/v1/{project_id}/dbss/audit/delete-job/{failed_id} | dbss::deleteAuditInstance-Job     | -          |
| GET /dbss/v2/{project_id}/audit/databases/rds                  | dbss::listRdsDb                   | -          |
| POST /dbss/v1/{project_id}/dbss/audit/rds-instance             | dbss::listRdsDb                   | -          |
| POST /dbss/v1/{project_id}/dbss/audit/guassDbInstance          | dbss::listRdsDb                   | -          |
| POST /dbss/v1/{project_id}/dbss/audit/instance/start           | dbss:auditInstance:instance Start | -          |
| POST /dbss/v1/{project_id}/dbss/audit/start-instance           | dbss:auditInstance:instance Start | -          |
| POST /dbss/v1/{project_id}/dbss/audit/instance/reboot          | dbss:auditInstance:reboot         | -          |
| POST /dbss/v1/{project_id}/dbss/audit/reboot-instance          | dbss:auditInstance:reboot         | -          |
| POST /dbss/v1/{project_id}/dbss/audit/instance/stop            | dbss:auditInstance:stop           | -          |
| POST /dbss/v1/{project_id}/dbss/audit/stop-instance            | dbss:auditInstance:stop           | -          |

| API                                                                               | Action                                 | Dependency |
|-----------------------------------------------------------------------------------|----------------------------------------|------------|
| POST /dbss/v1/{project_id}/dbss/{instance_id}/audit/upgrade                       | dbss:auditInstance:upgrade             | -          |
| GET /dbss/v1/{project_id}/dbss/audit/upgrade/status                               | dbss::queryUpgradeStatus               | -          |
| POST /dbss/v1/{project_id}/dbss/audit/securitygroup                               | dbss:auditInstance:updateSecurityGroup | -          |
| POST /dbss/v1/{project_id}/dbss/audit/update-securitygroup                        | dbss:auditInstance:updateSecurityGroup | -          |
| PUT /dbss/v1/{project_id}/dbss/audit/instances/{instance_id}                      | dbss:auditInstance:modifyAttribute     | -          |
| POST /dbss/v1/{project_id}/dbss/audit/update-instance/{instance_id}               | dbss:auditInstance:modifyAttribute     | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/operation/agent/{agent_id}/download | dbss:auditInstance:downloadAgent       | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/operation/download-agent/{agent_id} | dbss:auditInstance:downloadAgent       | -          |
| GET /dbss/v2/{project_id}/{instance_id}/audit/agents/{agent_id}                   | dbss:auditInstance:downloadAgent       | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/agent/switch                       | dbss:auditInstance:switchAgent         | -          |

| API                                                                              | Action                             | Dependency |
|----------------------------------------------------------------------------------|------------------------------------|------------|
| GET /dbss/v2/{project_id}/{instance_id}/audit/agents                             | dbss:auditInstance:listAgents      | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/agents/{db_id}                     | dbss:auditInstance:listAgents      | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/agents/{db_id}/{agent_id}       | dbss:auditInstance:deleteAgent     | -          |
| DELETE /dbss/v2/{project_id}/{instance_id}/audit/agents/{agent_id}               | dbss:auditInstance:deleteAgent     | -          |
| POST /dbss/v2/{project_id}/{instance_id}/audit/agents                            | dbss:auditInstance:addAgent        | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/agents                            | dbss:auditInstance:addAgent        | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/agent/add-agent                   | dbss:auditInstance:addAgent        | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/agent/{agent_id}                  | dbss:auditInstance:addAgent        | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}/preview        | dbss:auditInstance:previewReporter | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/{report_id}/preview-report | dbss:auditInstance:previewReporter | -          |

| API                                                                   | Action                                           | Dependency           |
|-----------------------------------------------------------------------|--------------------------------------------------|----------------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config   | dbss:auditInstance:setAlarmConfig                | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/config-email | dbss:auditInstance:configAlarmEmail              | -                    |
| GET /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config    | dbss:auditInstance:getAlarmConfig                | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/search-rules | dbss:auditInstance:listRiskRules                 | -                    |
| POST /dbss/v1/{project_id}/obs/upload-config                          | dbss:auditInstance:exportInstancesDatabaseConfig | -                    |
| POST /dbss/v1/charge/{project_id}/audit/period/order                  | dbss:auditInstance:createOnPeriod                | dbss::listCommonInfo |
| GET /dbss/v1/{project_id}/{instance_id}/audit/agent/get-agent         | dbss:auditInstance:listAgents                    | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/agent/del-agent        | dbss:auditInstance:deleteAgent                   | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/{sql_id}      | dbss:auditInstance:editSqlInjectRule             | -                    |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/rule/sql/{sql_id}    | dbss:auditInstance:deleteSqlInjectRule           | -                    |



| API                                                                            | Action                                  | Dependency           |
|--------------------------------------------------------------------------------|-----------------------------------------|----------------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/delete-rules     | dbss:auditInstance:deleteSensitiveRule  | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/list-rules            | dbss:auditInstance:listRiskRules        | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/delete-scope         | dbss:auditInstance:deleteAuditScopeRule | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/delete-risk           | dbss:auditInstance:deleteRiskRule       | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/del-backup               | dbss:auditInstance:deleteBackup         | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/status                   | dbss:auditInstance:listBackups          | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/auto-backup-template     | dbss:auditInstance:getBackupConfig      | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/edit-rule/{scope-id} | dbss:auditInstance:editAuditScopeRule   | -                    |
| GET /dbss/v1/{project_id}/dbss/audit/list-instances                            | dbss:auditInstance:instanceList         | -                    |
| POST /dbss/v1/{project_id}/dbss/audit/create-instance                          | dbss:auditInstance:createOnDemand       | dbss::listCommonInfo |

| API                                                                                           | Action                                      | Dependency           |
|-----------------------------------------------------------------------------------------------|---------------------------------------------|----------------------|
| POST /dbss/v2/{project_id}/dbss/audit/charge/period/order                                     | dbss:auditInstance:createOnPeriod           | dbss::listCommonInfo |
| GET /dbss/v2/{project_id}/dbss/audit/availability-zone                                        | dbss::listCommonInfo                        | -                    |
| GET /dbss/v2/{project_id}/audit/summary/{busi_type}/taskstatus                                | dbss::getauditInstances-SummaryTaskStatus   | -                    |
| GET /dbss/v1/{project_id}/audit/summary/info                                                  | dbss:auditInstance:listInstancesSummaryInfo | -                    |
| GET /dbss/v1/{project_id}/audit/summary/{busi_type}/taskstatus                                | dbss::getauditInstances-SummaryTaskStatus   | -                    |
| GET /dbss/v1/{project_id}/audit/risk/statistics                                               | dbss:auditInstance:listInstancesSummaryInfo | -                    |
| POST /dbss/v1/{project_id}/audit/summary/{busi_type}/taskstatus                               | dbss::updateAuditInstances-SummaryInfo      | -                    |
| POST /dbss/v1/{project_id}/{instance_id}/audit/reports/templates-topic/scheduler/config-task  | dbss:auditInstance:setReporterConfig        | -                    |
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/templates-topic/scheduler/{template_id} | dbss:auditInstance:getReporterConfig        | -                    |

| API                                                                       | Action                             | Dependency |
|---------------------------------------------------------------------------|------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config-topic | dbss:auditInstance:setAlarmConfig  | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-config-topic  | dbss:auditInstance:getAlarmConfig  | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/databases                  | dbss:auditInstance:addBareDatabase | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/databases        | dbss:auditInstance:addBareDatabase | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/create-database  | dbss:auditInstance:addBareDatabase | -          |
| GET /dbss/v1/{project_id}/{instance_id}/dbss/audit/databases              | dbss:auditInstance:listDatabases   | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/operation/databases         | dbss:auditInstance:listDatabases   | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/operation/list-databases    | dbss:auditInstance:listDatabases   | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/switch           | dbss:auditInstance:switchDatabase  | -          |

| API                                                                      | Action                                  | Dependency |
|--------------------------------------------------------------------------|-----------------------------------------|------------|
| POST /dbss/v2/{project_id}/{instance_id}/audit/databases/switch          | dbss:auditInstance:switchDatabase       | -          |
| DELETE /dbss/v2/{project_id}/{instance_id}/audit/databases/{db_id}       | dbss:auditInstance:deleteDatabase       | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/database/delete | dbss:auditInstance:deleteDatabase       | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/delete-database | dbss:auditInstance:deleteDatabase       | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes               | dbss:auditInstance:addAuditScopeRule    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/add-rule       | dbss:auditInstance:addAuditScopeRule    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scope/switch         | dbss:auditInstance:switchAuditScopeRule | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk                 | dbss:auditInstance:addRiskRule          | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/add-rule        | dbss:auditInstance:addRiskRule          | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/switch          | dbss:auditInstance:switchRiskRule       | -          |

| API                                                                                    | Action                                 | Dependency |
|----------------------------------------------------------------------------------------|----------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/{risk_id}                     | dbss:auditInstance:editRiskRule        | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/edit-risk/{risk_id}           | dbss:auditInstance:editRiskRule        | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes/{scope_id}                  | dbss:auditInstance:editAuditScopeRule  | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/email/{email_id}              | dbss:auditInstance:configAlarmEmail    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/edit-email/{email_id}         | dbss:auditInstance:configAlarmEmail    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/rank-risk                     | dbss:auditInstance:setRiskRulePriority | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rule/{rule_id}                 | dbss:auditInstance:editSqlInjectRule   | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/rule/sql-rule/{rule_id}               | dbss:auditInstance:deleteSqlInjectRule | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/reports/templates/scheduler/config-task | dbss:auditInstance:setReporterConfig   | -          |

| API                                                                                     | Action                                                 | Dependency |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/risk-statistics                  | dbss:auditInstance:listStatistics                      | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/session-statistics               | dbss:auditInstance:listStatistics                      | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/sql-statistics                   | dbss:auditInstance:listStatistics                      | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/reports/templates/scheduler/{template_id} | dbss:auditInstance:getReporterConfig                   | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/sqls/{sql_statement_id}                   | dbss:auditInstance:listSqls                            | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/result/switch                   | dbss:auditInstance:listSensitiveRules                  | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/switch                     | dbss:auditInstance:listSensitiveRules                  | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/result/switch                  | dbss:auditInstance:modifySensitiveRuleSaveResultSwitch | -          |

| API                                                                           | Action                                                | Dependency |
|-------------------------------------------------------------------------------|-------------------------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/switch          | dbss:auditInstance:modifySensitiveRuleAnonymizeSwitch | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/sensitive/masks/{rule_id}    | dbss:auditInstance:deleteSensitiveRule                | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/sensitive/mask/rule/switch     | dbss:auditInstance:switchSensitiveRule                | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/rule/scopes/{scope_id}       | dbss:auditInstance:deleteAuditScopeRule               | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/rule/risk/{risk_id}          | dbss:auditInstance:deleteRiskRule                     | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-log              | dbss:auditInstance:listAlarmItems                     | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/alarm-log                      | dbss:auditInstance:listAlarmItems                     | -          |
| PUT /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-log/{alarm_id}    | dbss:auditInstance:markAlarm                          | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/general/alarm-log/{alarm_id} | dbss:auditInstance:deleteAlarm                        | -          |

| API                                                                        | Action                             | Dependency |
|----------------------------------------------------------------------------|------------------------------------|------------|
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/mark-alarm-log      | dbss:auditInstance:markAlarm       | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/general/synopsis-statistics | dbss:auditInstance:listStatistics  | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backups                     | dbss:auditInstance:listBackups     | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/get-backup           | dbss:auditInstance:listBackups     | -          |
| DELETE /dbss/v1/{project_id}/{instance_id}/audit/backups/{id}              | dbss:auditInstance:deleteBackup    | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/restore              | dbss:auditInstance:restoreBackup   | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/retry                | dbss:auditInstance:retryBackup     | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/backup/bucket-name           | dbss:auditInstance:getBackupConfig | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/backup/status                | dbss:auditInstance:listBackups     | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/backup/auto-backup-template  | dbss:auditInstance:getBackupConfig | -          |



| API                                                                         | Action                                     | Dependency |
|-----------------------------------------------------------------------------|--------------------------------------------|------------|
| GET /dbss/v1/{project_id}/{instance_id}/audit/backup/risk-templates         | dbss:auditInstance:getRiskBackupConfigInfo | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/backup/risk-template/{db_id}  | dbss:auditInstance:getRiskBackupConfigInfo | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/risk/switch           | dbss:auditInstance:switchRiskBackup        | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/backup/risk-bucket-path       | dbss:auditInstance:getRiskBackupBucketInfo | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/backup/risk-bucket-path      | dbss:auditInstance:setRiskBackupBucketInfo | -          |
| GET /dbss/v1/{project_id}/{instance_id}/audit/backup/bucket-path            | dbss:auditInstance:getBackupConfig         | -          |
| POST /dbss/v1/{project_id}/{instance_id}/dbss/audit/databases/rds           | dbss:auditInstance:addRdsDatabase          | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/rds                | dbss:auditInstance:addRdsDatabase          | -          |
| POST /dbss/v1/{project_id}/{instance_id}/audit/operation/create-guassdb-rds | dbss:auditInstance:addRdsDatabase          | -          |

| API                                                                          | Action                                     | Dependency                         |
|------------------------------------------------------------------------------|--------------------------------------------|------------------------------------|
| POST /dbss/v2/{project_id}/{instance_id}/audit/databases/rds                 | dbss:auditInstance:addRdsDatabase          | -                                  |
| POST /dbss/v1/{domain_id}/{instance_id}/audit/backup/risk-bucket-path/global | dbss:auditInstance:setRiskBackupBucketInfo | -                                  |
| POST /dbss/v1/{domain_id}/{instance_id}/audit/backup/global/switch           | dbss:auditInstance:switchBackup            | dbss:auditInstance:getBackupConfig |
| POST /dbss/v1/{domain_id}/{instance_id}/audit/backup/risk/global/switch      | dbss:auditInstance:switchRiskBackup        | -                                  |
| GET /dbss/v1/{project_id}/dbss/server-info                                   | dbss::getServerInfo                        | -                                  |
| GET /dbss/v1/{project_id}/dbss/audit/jobs/{resource_id}                      | dbss::getAuditInstanceJob                  | -                                  |
| GET /dbss/v1/{project_id}/dbss/audit/list-jobs/{resource_id}                 | dbss::getAuditInstanceJob                  | -                                  |
| GET /dbss/v1/{project_id}/dbss/audit/list-jobs                               | dbss:auditInstance:listJobs                | -                                  |
| GET /dbss/v1/{project_id}/dbss/audit/specification                           | dbss::listCommonInfo                       | -                                  |
| GET /dbss/v1/{project_id}/dbss/audit/instances                               | dbss:auditInstance:instanceList            | -                                  |
| GET /dbss/v1/{project_id}/dbss/audit/quota                                   | dbss::listCommonInfo                       | -                                  |

| API                                                                                         | Action                                 | Dependency           |
|---------------------------------------------------------------------------------------------|----------------------------------------|----------------------|
| GET /dbss/v1/{project_id}/dbss/availability-zone                                            | dbss::listCommonInfo                   | -                    |
| GET /dbss/v1/{project_id}/dbss/get-availability-zone                                        | dbss::listCommonInfo                   | -                    |
| GET /dbss/v1/{project_id}/obs/audit/backup/obs-buckets                                      | dbss::listObsBuckets                   | -                    |
| POST /dbss/v1/{project_id}/dbss/audit/security-group                                        | dbss:auditInstance:updateSecurityGroup | -                    |
| POST /dbss/v1/{project_id}/dbss/audit/instances                                             | dbss:auditInstance:createOnDemand      | dbss::listCommonInfo |
| DELETE /dbss/v1/{project_id}/dbss/audit/delete-instance                                     | dbss:auditInstance:instanceDelete      | -                    |
| POST /dbss/v1/{project_id}/{resource_type}/resource-instances/filter                        | dbss::listResourcesByTag               | -                    |
| POST /dbss/v1/{project_id}/{resource_type}/resource-instances/count                         | dbss::listResourcesByTag               | -                    |
| POST /dbss/v1/{project_id}/{resource_type}/{resource_id}/tags/create                        | dbss::tagResource                      | -                    |
| DELETE dbss::listCommonInfo /dbss/v1/{project_id}/{resource_type}/{resource_id}/tags/delete | dbss::unTagResource                    | -                    |

| API                                                          | Action                    | Dependency |
|--------------------------------------------------------------|---------------------------|------------|
| GET /dbss/v1/{project_id}/{resource_type}/tags               | dbss::listTags            | -          |
| GET /dbss/v1/{project_id}/{resource_type}/{resource_id}/tags | dbss::listTagsForResource | -          |

## Resource

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-162](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DBSS.

**Table 3-162** Resource types supported by DBSS

| Resource Type | URN                                                    |
|---------------|--------------------------------------------------------|
| auditInstance | dbss:<region>:<account-id>:auditInstance:<instance-id> |

## Conditions

### Condition Key

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- Condition keys are the key values in the Condition element of an identity policy statement. Condition keys are classified into global condition keys and service-specific condition keys based on the application scope.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, dbss:) apply only to operations of the specific service. For details, see [Table 3-163](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the

request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.

- A condition operator, a condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by DBSS

The following table lists the condition keys that you can define in identity policies for DBSS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-163** Service-specific condition keys supported by DBSS

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Important Notes                                                            |
|--------------------------------|--------|-------------------------------|----------------------------------------------------------------------------|
| <code>dbss:VpcId</code>        | string | Single-valued                 | Filters access based on the network ID specified in the request parameter. |
| <code>dbss:SubnetId</code>     | string | Single-valued                 | Filters access based on the subnet ID specified in the request parameter.  |

## 3.7.7 Data Security Center (DSC)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DSC, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DSC, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DSC.

**Table 3-164** Actions supported by DSC

| Action                  | Description                                                           | Access Level          | Resource Type (*: required) | Condition Key | Alias |
|-------------------------|-----------------------------------------------------------------------|-----------------------|-----------------------------|---------------|-------|
| dsc:authorization:get   | Grants permission to query authorization status of cloud data assets. | permission_management | -                           | -             | -     |
| dsc:authorization:grant | Grants permission to authorize or deauthorize cloud data assets.      | permission_management | -                           | -             | -     |
| dsc:asset:delete        | Grants permission to delete data assets.                              | write                 | asset *                     | -             | -     |
| dsc:asset:list          | Grants permission to query data asset list.                           | list                  | asset *                     | -             | -     |
| dsc:asset:create        | Grants permission to create data assets.                              | write                 | asset *                     | -             | -     |
| dsc:asset:update        | Grants permission to update data asset info.                          | write                 | asset *                     | -             | -     |
| dsc:overview:list       | Grants permission to view data security overview.                     | list                  | -                           | -             | -     |
| dsc:maskTask:create     | Grants permission to create data masking tasks.                       | write                 | maskTask *                  | -             | -     |

| Action                    | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dsc:maskTask:update       | Grants permission to update data masking tasks.                                           | write        | mask Task *                 | -             | -     |
| dsc:maskTask:list         | Grants permission to query data masking tasks list.                                       | list         | mask Task *                 | -             | -     |
| dsc:maskTask:get          | Grants permission to query the detail of a data masking task.                             | read         | mask Task *                 | -             | -     |
| dsc:maskTask:delete       | Grants permission to delete data masking tasks.                                           | write        | mask Task *                 | -             | -     |
| dsc:maskTask:operate      | Grants permission to operate (such as start, stop, enable or disable) data masking tasks. | write        | mask Task *                 | -             | -     |
| dsc:maskTask:listSubTasks | Grants permission to query the subtask list of a data masking task.                       | list         | mask Task *                 | -             | -     |
| dsc:common:operate        | Grants permission to operate DSC general resources.                                       | write        | -                           | -             | -     |



| Action                   | Description                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dsc:scanTask:create      | Grants permission to create data scan tasks.                        | write        | scanTask *                  | -             | -     |
| dsc:scanTask:update      | Grants permission to update data scan tasks.                        | write        | scanTask *                  | -             | -     |
| dsc:scanTask:delete      | Grants permission to delete data scan tasks or subtasks.            | write        | scanTask *                  | -             | -     |
| dsc:scanTask:operate     | Grants permission to operate data scan tasks or subtasks.           | write        | scanTask *                  | -             | -     |
| dsc:scanTask:list        | Grants permission to query the list of data scan tasks or subtasks. | list         | scanTask *                  | -             | -     |
| dsc:scanRuleGroup:update | Grants permission to update info of scan rule groups.               | write        | -                           | -             | -     |
| dsc:scanRuleGroup:list   | Grants permission to query the list of scan rule groups.            | list         | -                           | -             | -     |
| dsc:scanRuleGroup:create | Grants permission to create scan rule groups.                       | write        | -                           | -             | -     |

| Action                   | Description                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dsc:scanRuleGroup:get    | Grants permission to query the detail of a scan rule group. | read         | -                           | -             | -     |
| dsc:scanRuleGroup:delete | Grants permission to delete scan rule groups.               | write        | -                           | -             | -     |
| dsc:scanRule:list        | Grants permission to query the list of scan rules.          | list         | scanRule *                  | -             | -     |
| dsc:scanRule:create      | Grants permission to create scan rules.                     | write        | scanRule *                  | -             | -     |
| dsc:scanRule:update      | Grants permission to update info of scan rules.             | write        | scanRule *                  | -             | -     |
| dsc:scanRule:get         | Grants permission to query the detail of a scan rule.       | read         | scanRule *                  | -             | -     |
| dsc:scanRule:delete      | Grants permission to delete scan rules.                     | write        | scanRule *                  | -             | -     |
| dsc:scanTask:getResults  | Grants permission to query the scan results of a scan task. | read         | scanTask *                  | -             | -     |

| Action                  | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dsc:common:list         | Grants permission to query DSC general resource list.                       | list         | -                           | -             | -     |
| dsc:sensitiveData:mask  | Grants permission to perform dynamic masking for sensitive data.            | write        | -                           | -             | -     |
| dsc:watermark:embed     | Grants permission to embed watermark into documents, images or databases.   | write        | -                           | -             | -     |
| dsc:watermark:extract   | Grants permission to extract watermark from documents, images or databases. | write        | -                           | -             | -     |
| dsc:scanTemplate:list   | Grants permission to query scan template list.                              | list         | scanTemplate *              | -             | -     |
| dsc:scanTemplate:create | Grants permission to create scan templates.                                 | write        | scanTemplate *              | -             | -     |
| dsc:scanTemplate:update | Grants permission to update scan templates.                                 | write        | scanTemplate *              | -             | -     |

| Action                  | Description                                              | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dsc:scanTemplate:delete | Grants permission to delete scan templates.              | write        | scanTemplate *              | -             | -     |
| dsc:scanTemplate:get    | Grants permission to query the detail of scan templates. | read         | scanTemplate *              | -             | -     |

Each API of DSC usually supports one or more actions. [Table 3-165](#) lists the supported actions and dependencies.

**Table 3-165** Actions and dependencies supported by DSC APIs

| API                                                     | Action             | Dependencies                |
|---------------------------------------------------------|--------------------|-----------------------------|
| DELETE/v1/{project_id}/sdg/asset/obs/bucket/{bucket_id} | dsc:asset:delete   | obs:bucket:GetBucketLogging |
|                                                         |                    | obs:bucket:PutBucketLogging |
| GET/v1/{project_id}/sdg/asset/obs/buckets               | dsc:asset:list     | obs:bucket:listAllMyBuckets |
| POST/v1/{project_id}/sdg/asset/obs/buckets              | dsc:asset:create   | obs:bucket:GetBucketStorage |
|                                                         |                    | obs:bucket:listAllMyBuckets |
| PUT/v1/{project_id}/sdg/asset/{asset_id}/name           | dsc:asset:update   | -                           |
| POST/v1/{project_id}/period/order                       | dsc:common:operate | bss:renewal:update          |
|                                                         |                    | bss:order:update            |
| GET/v1/{project_id}/period/product/specification        | dsc:common:list    | -                           |

| API                                                                        | Action                    | Dependencies   |
|----------------------------------------------------------------------------|---------------------------|----------------|
| POST/v1/{project_id}/sdg/server/mask/dbs/templates/{template_id}/operation | dsc:maskTask:operate      | -              |
| GET/v1/{project_id}/sdg/server/mask/dbs/templates/{template_id}/tasks      | dsc:maskTask:listSubTasks | -              |
| PUT/v1/{project_id}/sdg/smn/topic                                          | dsc:common:operate        | -              |
| GET/v1/{project_id}/sdg/smn/topics                                         | dsc:common:list           | smn:topic:list |
| GET/v1/{project_id}/openapi/called-records                                 | dsc:common:list           | -              |
| POST/v1/{project_id}/sdg/scan/job                                          | dsc:scanTask:create       | -              |
| GET/v1/{project_id}/sdg/scan/jobs                                          | dsc:scanTask:list         | -              |
| GET/v1/{project_id}/sdg/server/scan/groups                                 | dsc:scanRuleGroup:list    | -              |
| POST/v1/{project_id}/sdg/server/scan/groups                                | dsc:scanRuleGroup:create  | -              |
| DELETE/v1/{project_id}/sdg/server/scan/groups/{group_id}                   | dsc:scanRuleGroup:delete  | -              |
| GET/v1/{project_id}/sdg/server/scan/rules                                  | dsc:scanRule:list         | -              |
| POST/v1/{project_id}/sdg/server/scan/rules                                 | dsc:scanRule:create       | -              |

| API                                                                                          | Action                  | Dependencies |
|----------------------------------------------------------------------------------------------|-------------------------|--------------|
| PUT/v1/<br>{project_id}/sdg/<br>server/scan/rules                                            | dsc:scanRule:update     | -            |
| DELETE/v1/<br>{project_id}/sdg/<br>server/scan/rules/<br>{rule_id}                           | dsc:scanRule:delete     | -            |
| GET/v1/<br>{project_id}/sdg/<br>scan/job/{job_id}/<br>results                                | dsc:scanTask:getResults | -            |
| GET/v1/<br>{project_id}/sdg/<br>server/relation/jobs/<br>{job_id}/dbs                        | dsc:common:list         | -            |
| GET/v1/<br>{project_id}/sdg/<br>server/relation/jobs/<br>{job_id}/dbs/<br>{db_id}/tables     | dsc:common:list         | -            |
| GET/v1/<br>{project_id}/sdg/<br>server/relation/jobs/<br>{job_id}/dbs/<br>{table_id}/columns | dsc:common:list         | -            |
| GET/v1/<br>{project_id}/sdg/<br>server/relation/jobs/<br>{job_id}/obs/<br>buckets            | dsc:common:list         | -            |
| GET/v1/<br>{project_id}/sdg/<br>server/relation/jobs/<br>{job_id}/obs/<br>{bucket_id}/files  | dsc:common:list         | -            |
| POST/v1/<br>{project_id}/data/<br>mask                                                       | dsc:sensitiveData:mask  | -            |
| POST/v1/<br>{project_id}/doc-<br>address/watermark/<br>embed                                 | dsc:watermark:embed     | -            |

| API                                                        | Action                | Dependencies |
|------------------------------------------------------------|-----------------------|--------------|
| POST/v1/{project_id}/doc-address/watermark/extract         | dsc:watermark:extract | -            |
| POST/v1/{project_id}/image-address/watermark/embed         | dsc:watermark:embed   | -            |
| POST/v1/{project_id}/image-address/watermark/extract       | dsc:watermark:extract | -            |
| POST/v1/{project_id}/image-address/watermark/extract-image | dsc:watermark:extract | -            |
| POST/v1/{project_id}/image/watermark/embed                 | dsc:watermark:embed   | -            |
| POST/v1/{project_id}/image/watermark/extract               | dsc:watermark:extract | -            |
| POST/v1/{project_id}/image/watermark/extract-image         | dsc:watermark:extract | -            |
| POST/v1/{project_id}/sdg/database/watermark/embed          | dsc:watermark:embed   | -            |
| POST/v1/{project_id}/sdg/database/watermark/extract        | dsc:watermark:extract | -            |
| POST/v1/{project_id}/sdg/doc/watermark/embed               | dsc:watermark:embed   | -            |
| POST/v1/{project_id}/sdg/doc/watermark/extract             | dsc:watermark:extract | -            |

| API                                                          | Action                | Dependencies |
|--------------------------------------------------------------|-----------------------|--------------|
| GET/v1/{project_id}/sdg/asset/{asset_type}/{asset_id}/detail | dsc:common:list       | -            |
| GET /v1/{project_id}/sdg/asset/authorization                 | dsc:authorization:get | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-166](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DSC.

**Table 3-166** Resource types supported by DSC

| Resource Type | URN                                                  |
|---------------|------------------------------------------------------|
| scanTask      | dsc:<region>:<account-id>:scanTask:<task-id>         |
| scanRule      | dsc:<region>:<account-id>:scanRule:<rule-id>         |
| scanTemplate  | dsc:<region>:<account-id>:scanTemplate:<template-id> |
| maskTask      | dsc:<region>:<account-id>:maskTask:<task-id>         |
| asset         | dsc:<region>:<account-id>:asset:<asset-id>           |

## Conditions

DSC does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.7.8 Web Application Firewall (WAF)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.



SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by waf, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by waf, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for waf.

**Table 3-167** Actions supported by waf

| Action           | Description                                             | Access Level | Resource Type (*: required) | Condition Key                         | Alias                 |
|------------------|---------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------|
| waf:host:list    | Grants permission to query all protected domain names.  | List         | host *                      | -                                     | • waf:instance:list   |
|                  |                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                       |
| waf:host:create  | Grants permission to create a protection domain name.   | Write        | host *                      | -                                     | • waf:instance:create |
|                  |                                                         |              | policy                      | -                                     |                       |
|                  |                                                         |              | certificate                 | -                                     |                       |
|                  |                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                       |
| waf:host:get     | Grants permission to query the protected domain name.   | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | • waf:instance:get    |
| waf:host:put     | Grants permission to update the protected domain name.  | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | • waf:instance:put    |
|                  |                                                         |              | certificate                 | -                                     |                       |
| waf:host:delete  | Grants permission to delete the protection domain name. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | • waf:instance:delete |
| waf:sourcelp:get | Grants permission to query WAF IP addresses.            | Read         | -                           | -                                     | -                     |

| Action            | Description                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                 |
|-------------------|------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------|
| waf:policy:list   | Grants permission to query all protected policies.         | List         | policy *                    | -                                     | -                                                                     |
|                   |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                       |
| waf:policy:create | Grants permission to create a protection policy.           | Write        | policy *                    | -                                     | -                                                                     |
|                   |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                       |
| waf:policy:get    | Grants permission to query the protected policy.           | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                     |
| waf:policy:put    | Grants permission to update the protected policy.          | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                     |
|                   |                                                            |              | host                        | -                                     |                                                                       |
| waf:policy:delete | Grants permission to delete the protection policy.         | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                     |
| waf:ccRule:list   | Grants permission to query all CC attack protection rules. | List         | policy *                    | -                                     | <ul style="list-style-type: none"> <li>waf:ccRuleRule:list</li> </ul> |
|                   |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                       |
| waf:ccRule:create | Grants permission to create a CC attack protection rule.   | Write        | policy *                    | -                                     | -                                                                     |
|                   |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                       |

| Action                           | Description                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                |
|----------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------|
| waf:ccRule:get                   | Grants permission to query the CC attack protection rule.  | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                    |
| waf:ccRule:put                   | Grants permission to update the CC attack rule.            | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>waf:ccRuleRule:put</li> </ul> |
| waf:ccRule:delete                | Grants permission to delete the CC attack protection rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                    |
| waf:preciseProtectionRule:list   | Grants permission to query all precise protection rules.   | List         | policy *                    | -                                     | -                                                                    |
|                                  |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                      |
| waf:preciseProtectionRule:create | Grants permission to create a precise protection rule.     | Write        | policy *                    | -                                     | -                                                                    |
|                                  |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                      |
| waf:preciseProtectionRule:get    | Grants permission to query the precise protection rule.    | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                    |
| waf:preciseProtectionRule:put    | Grants permission to update the precise protection rule.   | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                    |

| Action                           | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:preciseProtectionRule:delete | Grants permission to delete the precise protection rule.      | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:whiteBlacklistRule:list      | Grants permission to query all blacklist and whitelist rules. | List         | policy *                    | -                                     | -     |
|                                  |                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:whiteBlacklistRule:create    | Grants permission to create a blacklist and whitelist rule.   | Write        | policy *                    | -                                     | -     |
|                                  |                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:whiteBlacklistRule:get       | Grants permission to query the blacklist and whitelist rule.  | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:whiteBlacklistRule:put       | Grants permission to update the blacklist and whitelist rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:whiteBlacklistRule:delete    | Grants permission to delete the blacklist and whitelist rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:privacyRule:list             | Grants permission to query all data masking rules.            | List         | policy *                    | -                                     | -     |
|                                  |                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:privacyRule:create           | Grants permission to create a data masking rule.              | Write        | policy *                    | -                                     | -     |

| Action                        | Description                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                            |
|-------------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------------------|
|                               |                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                                  |
| waf:privacyRule:get           | Grants permission to query the data masking rule.         | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                                |
| waf:privacyRule:put           | Grants permission to update the data masking rule.        | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                                |
| waf:privacyRule:delete        | Grants permission to delete the data masking rule.        | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                                |
| waf:falseAlarmMaskRule:list   | Grants permission to query all false alarm masking rules. | List         | policy *                    | -                                     | -                                                                                |
|                               |                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                                  |
| waf:falseAlarmMaskRule:create | Grants permission to create a false alarm masking rule.   | Write        | policy *                    | -                                     | -                                                                                |
|                               |                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                                  |
| waf:falseAlarmMaskRule:get    | Grants permission to query the false alarm masking rule.  | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -                                                                                |
| waf:falseAlarmMaskRule:put    | Grants permission to update the false alarm masking rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>waf:falseAlarmMaskRule:recount</li> </ul> |

| Action                        | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|-------------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:falseAlarmMaskRule:delete | Grants permission to delete the false alarm masking rule.        | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:geolpRule:list            | Grants permission to query all geolocation access control rules. | List         | policy *                    | -                                     | -     |
|                               |                                                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:geolpRule:create          | Grants permission to create a geolocation access control rule.   | Write        | policy *                    | -                                     | -     |
|                               |                                                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:geolpRule:get             | Grants permission to query the geolocation access control rule.  | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:geolpRule:put             | Grants permission to update the geolocation access control rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:geolpRule:delete          | Grants permission to delete the geolocation access control rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:antiTamperRule:list       | Grants permission to query all web tamper protection rules.      | List         | policy *                    | -                                     | -     |
|                               |                                                                  |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |

| Action                     | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:antiTamperRule:create  | Grants permission to create a web tamper protection rule.                      | Write        | policy *                    | -                                     | -     |
|                            |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:antiTamperRule:get     | Grants permission to query the web tamper protection rule.                     | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:antiTamperRule:put     | Grants permission to update the web tamper protection rule.                    | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:antiTamperRule:delete  | Grants permission to delete the web tamper protection rule.                    | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:antiLeakageRule:list   | Grants permission to query all information leakage prevention rules.           | List         | policy *                    | -                                     | -     |
|                            |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:antiLeakageRule:create | Grants permission to create the sensitive information leakage prevention rule. | Write        | policy *                    | -                                     | -     |
|                            |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |



| Action                     | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:antiLeakageRule:get    | Grants permission to query the information leakage prevention rule.            | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:antiLeakageRule:put    | Grants permission to update the information leakage prevention rule.           | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:antiLeakageRule:delete | Grants permission to delete the sensitive information leakage prevention rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:anticrawlerRule:list   | Grants permission to query all anti-crawler protection rules.                  | List         | policy *                    | -                                     | -     |
|                            |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:anticrawlerRule:create | Grants permission to create the anti-crawler protection rule.                  | Write        | policy *                    | -                                     | -     |
|                            |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:anticrawlerRule:get    | Grants permission to query the anti-crawler protection rule.                   | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |

| Action                     | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:anticrawlerRule:put    | Grants permission to update the anti-crawler protection rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:anticrawlerRule:delete | Grants permission to delete the anti-crawler protection rule. | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:punishmentRule:list    | Grants permission to query all known attack source rules.     | List         | policy *                    | -                                     | -     |
|                            |                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:punishmentRule:create  | Grants permission to create the known attack source rule.     | Write        | policy *                    | -                                     | -     |
|                            |                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:punishmentRule:get     | Grants permission to query the known attack source rule.      | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:punishmentRule:put     | Grants permission to update the known attack source rule.     | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:punishmentRule:delete  | Grants permission to delete the known attack source rule.     | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:valueList:list         | Grants permission to query all valuelists.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |

| Action               | Description                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------|---------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:valuelist:create | Grants permission to create valuelist.            | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:valuelist:get    | Grants permission to query the valuelist.         | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:valuelist:put    | Grants permission to update the valuelist.        | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:valuelist:delete | Grants permission to delete the valuelist.        | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:ipgroup:list     | Grants permission to list of IP address groups.   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:ipgroup:create   | Grants permission to create IP address group.     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:ipgroup:get      | Grants permission to get IP address group detail. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:ipgroup:put      | Grants permission to modify IP address group.     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:ipgroup:delete   | Grants permission to delete IP address group.     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |

| Action                     | Description                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:certificate:list       | Grants permission to query all certificates.               | List         | certificate *               | -                                     | -     |
|                            |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:certificate:create     | Grants permission to create a certificate.                 | Write        | certificate *               | -                                     | -     |
|                            |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:certificate:get        | Grants permission to query the certificate.                | Read         | certificate *               | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:certificate:put        | Grants permission to modify certificate.                   | Write        | certificate *               | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:certificate:delete     | Grants permission to delete the certificate.               | Write        | certificate *               | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:certificate:apply      | Grants permission to apply certificate to hosts.           | Write        | certificate *               | <a href="#">g:EnterpriseProjectId</a> | -     |
|                            |                                                            |              | host *                      | -                                     |       |
| waf:premiuminstance:list   | Grants permission to query all dedicated engine instances. | List         | premiuminstance *           | -                                     | -     |
|                            |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| waf:premiuminstance:create | Grants permission to create a dedicated engine instance.   | Write        | premiuminstance *           | -                                     | -     |

| Action                     | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|----------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                            |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| waf:premiumInstance:get    | Grants permission to query the dedicated engine instance.  | Read         | premiumInstance *           | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -     |
| waf:premiumInstance:put    | Grants permission to update the dedicated engine instance. | Write        | premiumInstance *           | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -     |
| waf:premiumInstance:delete | Grants permission to delete the dedicated engine instance. | Write        | premiumInstance *           | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -     |
| waf:event:get              | Grants permission to query the protection event.           | Read         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| waf:lbsConfig:get          | Grants permission to query the lbsConfig.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| waf:lbsConfig:put          | Grants permission to update the lbsConfig.                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |

| Action                | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|-----------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| waf:postpaid:create   | Grants permission to create the postpaid.               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| waf:postpaid:delete   | Grants permission to delete the postpaid.               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| waf:prepaid:create    | Grants permission to create a prepaid order.            | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -     |
| waf:subscription:get  | Grants permission to query the cloud mode subscription. | Read         | -                           | -                                                                                                                                                                                      | -     |
| waf:alert:get         | Grants permission to query the alertConfig.             | List         | -                           | -                                                                                                                                                                                      | -     |
| waf:alert:put         | Grants permission to update the alertConfig.            | Write        | -                           | -                                                                                                                                                                                      | -     |
| waf:consoleConfig:get | Grants permission to query the console configurations.  | Read         | -                           | -                                                                                                                                                                                      | -     |
| waf:bundle:get        | Grants permission to query the user bundle.             | Read         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |

| Action                              | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|-------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| waf:securityReportSubscription:list | Grants permission to query the security report subscription. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| waf:tmsProjectTags:get              | Grants permission to query the tms project tags.             | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |

Each API of waf usually supports one or more actions. [Table 3-168](#) lists the supported actions and dependencies.

**Table 3-168** Actions and dependencies supported by waf APIs

| API                                                   | Action          | Dependencies |
|-------------------------------------------------------|-----------------|--------------|
| POST /v1/{project_id}/waf/instance                    | waf:host:create | -            |
| DELETE /v1/{project_id}/waf/instance/{instance_id}    | waf:host:delete | -            |
| GET /v1/{project_id}/waf/instance                     | waf:host:list   | -            |
| GET /v1/{project_id}/waf/instance/{instance_id}/route | waf:host:get    | -            |
| GET /v1/{project_id}/waf/instance/{instance_id}       | waf:host:get    | -            |

| API                                                            | Action            | Dependencies |
|----------------------------------------------------------------|-------------------|--------------|
| PATCH /v1/{project_id}/waf/instance/{instance_id}              | waf:host:put      | -            |
| PUT /v1/{project_id}/waf/instance/{instance_id}/protect-status | waf:host:put      | -            |
| POST /v1/{project_id}/premium-waf/host                         | waf:host:create   | -            |
| DELETE /v1/{project_id}/premium-waf/host/{host_id}             | waf:host:delete   | -            |
| GET /v1/{project_id}/premium-waf/host                          | waf:host:list     | -            |
| GET /v1/{project_id}/premium-waf/host/{host_id}                | waf:host:get      | -            |
| PUT /v1/{project_id}/premium-waf/host/{host_id}                | waf:host:put      | -            |
| PUT /v1/{project_id}/premium-waf/host/{host_id}/protect-status | waf:host:put      | -            |
| POST /v1/{project_id}/waf/policy                               | waf:policy:create | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}                 | waf:policy:delete | -            |
| GET /v1/{project_id}/waf/policy                                | waf:policy:list   | -            |



| API                                                      | Action                            | Dependencies |
|----------------------------------------------------------|-----------------------------------|--------------|
| GET /v1/{project_id}/waf/policy/{policy_id}              | waf:policy:get                    | -            |
| PATCH /v1/{project_id}/waf/policy/{policy_id}            | waf:policy:put                    | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}              | waf:policy:put                    | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/cc          | waf:ccRule:create                 | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/custom      | waf:preciseProtection-Rule:create | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/antitamper  | waf:antiTamperRule:create         | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/antileakage | waf:antiLeakageRule:create        | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/anticrawler | waf:anticrawlerRule:create        | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/punishment  | waf:punishmentRule:create         | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/geoup       | waf:geoupRule:create              | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/ignore      | waf:falseAlarmMaskRule:create     | -            |

| API                                                                  | Action                           | Dependencies |
|----------------------------------------------------------------------|----------------------------------|--------------|
| POST /v1/{project_id}/waf/policy/{policy_id}/privacy                 | waf:privacyRule:create           | -            |
| POST /v1/{project_id}/waf/valuelist                                  | waf:valueList:create             | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/whiteblackip            | waf:whiteBlackIpRule:create      | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}          | waf:ccRule:delete                | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}      | waf:preciseProtectionRule:delete | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}  | waf:antiTamperRule:delete        | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id} | waf:antiLeakageRule:delete       | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id} | waf:anticrawlerRule:delete       | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}  | waf:punishmentRule:delete        | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}       | waf:geoIpRule:delete             | -            |

| API                                                                   | Action                         | Dependencies |
|-----------------------------------------------------------------------|--------------------------------|--------------|
| DELETE /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}       | waf:falseAlarmMaskRule:delete  | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}      | waf:privacyRule:delete         | -            |
| DELETE /v1/{project_id}/waf/valuelist/{valuelistid}                   | waf:valueList:delete           | -            |
| DELETE /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id} | waf:whiteBlackIpRule:delete    | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/custom                    | waf:preciseProtectionRule:list | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/cc                        | waf:ccRule:list                | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/antitamper                | waf:antiTamperRule:list        | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/antileakage               | waf:antiLeakageRule:list       | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler               | waf:anticrawlerRule:list       | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/punishment                | waf:punishmentRule:list        | -            |

| API                                                                       | Action                        | Dependencies |
|---------------------------------------------------------------------------|-------------------------------|--------------|
| GET /v1/{project_id}/waf/policy/{policy_id}/geoip                         | waf:geoIpRule:list            | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/ignore                        | waf:falseAlarmMaskRule:list   | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/privacy                       | waf:privacyRule:list          | -            |
| GET /v1/{project_id}/waf/valuelist                                        | waf:valueList:list            | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip                  | waf:whiteBlackIpRule:list     | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}                  | waf:ccRule:put                | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}              | waf:preciseProtectionRule:put | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}               | waf:geoIpRule:put             | -            |
| POST /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}/refresh | waf:antiTamperRule:put        | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}         | waf:antiLeakageRule:put       | -            |

| API                                                                     | Action                     | Dependencies |
|-------------------------------------------------------------------------|----------------------------|--------------|
| PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}       | waf:anticrawlerRule:put    | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/anticrawler                 | waf:anticrawlerRule:put    | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}        | waf:punishmentRule:put     | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/{ruletype}/{rule_id}/status | waf:whiteBlackIpRule:put   | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}           | waf:privacyRule:put        | -            |
| PUT /v1/{project_id}/waf/valuelist/{valuelistid}                        | waf:valueList:put          | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id}      | waf:whiteBlackIpRule:put   | -            |
| PUT /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}            | waf:falseAlarmMaskRule:put | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/cc/{rule_id}                | waf:ccRule:get             | -            |

| API                                                                | Action                         | Dependencies |
|--------------------------------------------------------------------|--------------------------------|--------------|
| GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}       | waf:preciseProtection-Rule:get | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/whiteblackip/{rule_id} | waf:whiteBlackIpRule:get       | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/privacy/{rule_id}      | waf:privacyRule:get            | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/ignore/{rule_id}       | waf:falseAlarmMaskRule:get     | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}        | waf:geoIpRule:get              | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/antitamper/{rule_id}   | waf:antiTamperRule:get         | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}  | waf:antiLeakageRule:get        | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/anticrawler/{rule_id}  | waf:anticrawlerRule:get        | -            |
| GET /v1/{project_id}/waf/policy/{policy_id}/punishment/{rule_id}   | waf:punishmentRule:get         | -            |

| API                                                                   | Action                 | Dependencies |
|-----------------------------------------------------------------------|------------------------|--------------|
| GET /v1/{project_id}/waf/valuelist/{valuelistid}                      | waf:valuelist:get      | -            |
| POST /v1/{project_id}/waf/ip-groups                                   | waf:ipgroup:create     | -            |
| DELETE /v1/{project_id}/waf/ip-group/{id}                             | waf:ipgroup:delete     | -            |
| GET /v1/{project_id}/waf/ip-groups                                    | waf:ipgroup:list       | -            |
| GET /v1/{project_id}/waf/ip-group/{id}                                | waf:ipgroup:get        | -            |
| PUT /v1/{project_id}/waf/ip-group/{id}                                | waf:ipgroup:put        | -            |
| POST /v1/{project_id}/waf/certificate/{certificate_id}/apply-to-hosts | waf:certificate:apply  | -            |
| POST /v1/{project_id}/waf/certificate                                 | waf:certificate:create | -            |
| DELETE /v1/{project_id}/waf/certificate/{certificate_id}              | waf:certificate:delete | -            |
| GET /v1/{project_id}/waf/certificate                                  | waf:certificate:list   | -            |
| GET /v1/{project_id}/waf/certificate/{certificate_id}                 | waf:certificate:get    | -            |
| PUT /v1/{project_id}/waf/certificate/{certificate_id}                 | waf:certificate:put    | -            |

| API                                                        | Action                     | Dependencies |
|------------------------------------------------------------|----------------------------|--------------|
| GET /v1/{project_id}/waf/event                             | waf:event:get              | -            |
| GET /v1/{project_id}/waf/event/{eventid}                   | waf:event:get              | -            |
| GET /v1/{project_id}/waf/overviews/bandwidth/timeline      | waf:event:get              | -            |
| GET /v1/{project_id}/waf/overviews/classification          | waf:event:get              | -            |
| GET /v1/{project_id}/waf/overviews/qps/timeline            | waf:event:get              | -            |
| GET /v1/{project_id}/waf/overviews/request/timeline        | waf:event:get              | -            |
| GET /v1/{project_id}/waf/overviews/statistics              | waf:event:get              | -            |
| GET /v1/{project_id}/waf/overviews/abnormal                | waf:event:get              | -            |
| GET /v1/{project_id}/waf/config/console                    | waf:consoleConfig:get      | -            |
| POST /v1/{project_id}/premium-waf/instance                 | waf:premiumInstance:create | -            |
| DELETE /v1/{project_id}/premium-waf/instance/{instance_id} | waf:premiumInstance:delete | -            |



| API                                                                 | Action                   | Dependencies |
|---------------------------------------------------------------------|--------------------------|--------------|
| GET /v1/{project_id}/premium-waf/instance                           | waf:premiumInstance:list | -            |
| PUT /v1/{project_id}/premium-waf/instance/{instance_id}             | waf:premiumInstance:put  | -            |
| GET /v1/{project_id}/premium-waf/instance/{instance_id}             | waf:premiumInstance:get  | -            |
| GET /v1/{project_id}/waf/config/lts                                 | waf:ltsConfig:get        | -            |
| PUT /v1/{project_id}/waf/config/lts/{ltsconfig_id}                  | waf:ltsConfig:put        | -            |
| POST /v1/{project_id}/waf/subscription/batchalter/prepaid-cloud-waf | waf:prepaid:create       | -            |
| POST /v1/{project_id}/waf/subscription/purchase/prepaid-cloud-waf   | waf:prepaid:create       | -            |
| GET /v1/{project_id}/waf/subscription                               | waf:subscription:get     | -            |
| POST /v1/{project_id}/waf/postpaid                                  | waf:postpaid:create      | -            |
| DELETE /v1/{project_id}/waf/postpaid                                | waf:postpaid:delete      | -            |
| GET /v2/{project_id}/waf/alerts                                     | waf:alert:get            | -            |

| API                                                                            | Action                              | Dependencies |
|--------------------------------------------------------------------------------|-------------------------------------|--------------|
| PUT /v2/<br>{project_id}/waf/<br>alert/{alert_id}                              | waf:alert:put                       | -            |
| GET /v1/<br>{project_id}/waf/<br>config/source-ip                              | waf:sourcelp:get                    | -            |
| POST /v1/<br>{project_id}/<br>composite-waf/<br>hosts/migration                | waf:host:create                     | -            |
| GET /v1/<br>{project_id}/<br>composite-waf/host                                | waf:host:list                       | -            |
| GET /v1/<br>{project_id}/<br>composite-waf/<br>host/{host_id}                  | waf:host:get                        | -            |
| GET /v1/<br>{project_id}/waf/<br>bundle                                        | waf:bundle:get                      | -            |
| GET /v1/<br>{project_id}/waf/<br>security-report/<br>subscriptions             | waf:securityReportSubscription:list | -            |
| GET /v1/<br>{project_id}/waf/<br>overviews/attack/<br>action-types             | waf:event:get                       | -            |
| GET /v1/<br>{project_id}/waf/<br>policy/basic-<br>protection/default-<br>rules | waf:policy:get                      | -            |
| GET /v1/<br>{project_id}/waf/tag<br>/geoip/map                                 | waf:geoIpRule:get                   | -            |
| -                                                                              | waf:policy:get                      | -            |
| -                                                                              | waf:policy:get                      | -            |
| -                                                                              | waf:policy:get                      | -            |
| -                                                                              | waf:policy:get                      | -            |
| -                                                                              | waf:policy:get                      | -            |

| API | Action         | Dependencies |
|-----|----------------|--------------|
| -   | waf:policy:get | -            |
| -   | waf:policy:get | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-169](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for waf.

**Table 3-169** Resource types supported by waf

| Resource Type   | URN                                                     |
|-----------------|---------------------------------------------------------|
| policy          | waf:<region>:<account-id>;policy:<policy-id>            |
| host            | waf:<region>:<account-id>;host:<host-id>                |
| premiumInstance | waf:<region>:<account-id>;premiumInstance:<instance-id> |
| certificate     | waf:<region>:<account-id>;certificate:<certificate-id>  |

## Conditions

waf does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.7.9 Host Security Service (HSS)

#### Actions Supported by Identity Policy-based Authorization

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that

OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by HSS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by HSS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for HSS.

**Table 3-170** Actions supported by HSS

| Action                              | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|-------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:host:addHostsGroup              | Grants permission to create a server group.                                   | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:set</li> </ul>               |
| hss:ars:addPWLPolicyHost            | Grants permission to add servers to a whitelist policy.                       | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>                     |
| hss:rasp:addRaspPolicy              | Grants permission to add protection policies.                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:set</li> </ul>                    |
| hss:safetyReport:addSecurityReport  | Grants permission to create or copy new reports.                              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:set</li> </ul>            |
| hss:wtp:addTimingOffConfigInfo      | Grants permission to add the configuration of scheduled protection disabling. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpScheduledProtections:set</li> </ul> |
| hss:wtp:addWtpHostProtectDirInfo    | Grants permission to add protected directories.                               | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectories:set</li> </ul>          |
| hss:wtp:addWtpPrivilegedProcessInfo | Grants permission to add privileged processes.                                | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpPrivilegedProcess:set</li> </ul>    |

| Action                                 | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                       |
|----------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------|
| hss:setting:changeAutoKillVirusStatus  | Grants permission to enable or disable automatic program isolation and killing.       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:automaticKillMp:set</li> </ul>   |
| hss:event:changeBlockedIp              | Grants permission to unblock objects.                                                 | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:accountCracks:unblock</li> </ul> |
| hss:setting:changeMalwareCollectStatus | Grants permission to enable or disable the sample collection for malware cloud scans. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:automaticKillMp:set</li> </ul>   |
| hss:ars:changePWLPolicy                | Grants permission to modify whitelist policies.                                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>               |
| hss:ars:changePWLPolicyProcessStatus   | Grants permission to mark the whitelist policy identification processes.              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>               |
| hss:safetyReport:changeSecurityReport  | Grants permission to modify reports.                                                  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:set</li> </ul>      |
| hss:ars:createPWLPolicy                | Grants permission to create whitelist policies.                                       | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>               |
|                                        |                                                                                       |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                             |

| Action                                               | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|------------------------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:ars:delete PWLPolicy                             | Grants permission to delete whitelist policies.                                  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>                     |
| hss:ars:delete PWLPolicyHost                         | Grants permission to delete servers from a whitelist policy.                     | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>                     |
| hss:antiransomware:delete RansomwareDuplicationInfo  | Grants permission to delete backup copies.                                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>          |
| hss:antiransomware:delete RansomwareProtectionPolicy | Grants permission to delete protection policies.                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>          |
| hss:rasp:delete RaspPolicy                           | Grants permission to delete protection policies.                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:set</li> </ul>                    |
| hss:safetyReport:deleteSecurityReport                | Grants permission to delete reports.                                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:set</li> </ul>            |
| hss:wtp:delete TimingOffConfigInfo                   | Grants permission to delete the configuration of scheduled protection disabling. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpScheduledProtections:set</li> </ul> |
| hss:wtp:delete WtpBackupHostInfo                     | Grants permission to delete the remote backup server.                            | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpBackup:set</li> </ul>               |

| Action                                 | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                          |
|----------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------------|
| hss:wtp:deleteWtpHostProtectDirInfo    | Grants permission to delete protected directories.                                 | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectory:set</li> </ul>         |
| hss:wtp:deleteWtpPrivilegedProcessInfo | Grants permission to delete privileged processes.                                  | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpPrivilegedProcess:set</li> </ul> |
| hss:setting:getAgentInstallScript      | Grants permission to query the agent installation script.                          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:installAgent:get</li> </ul>         |
| hss:setting:getAlarmConfig             | Grants permission to query alarm configurations.                                   | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:alertConfig:get</li> </ul>          |
| hss:rasp:getAppRaspSwitchStatus        | Grants permission to query application protection status (enabled or disabled).    | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:list</li> </ul>                |
| hss:setting:getAutoKillVirusStatus     | Grants permission to query the automatic isolation and killing status of programs. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:automaticKillMp:get</li> </ul>      |



| Action                                         | Description                                                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:container:getContainerNodeStatistics       | Grants permission to query container node protection overview statistics.                                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul>     |
| hss:keyfile:getFileStatistic                   | Grants permission to obtain server file statistics.                                                          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:keyfiles:list</li> </ul>       |
| hss:setting:getMalwareCollectStatus            | Grants permission to query the status of the sample collection configuration switch for malware cloud scans. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:automaticKillMp:get</li> </ul> |
| hss:setting:getMalwareReminders                | Grants permission to obtain prompt information configurations.                                               | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:automaticKillMp:get</li> </ul> |
| hss:securitycheck:getManualSecurityCheckStatus | Grants permission to query the status and progress of manual health checks.                                  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:list</li> </ul>  |

| Action                                        | Description                                                                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:overview:getOverviewAssetGroupsStatistics | Grants permission to obtain business group distribution statistics and identify regular, important, and core assets. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewAssetOsStatistics     | Grants permission to obtain operating system distribution statistics.                                                | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewAssetStatistics       | Grants permission to obtain asset statistics, including servers, containers, and images.                             | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewAttackMitre           | Grants permission to investigate responses (ATT&CK attack path matrix).                                              | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewDefenseStatistics     | Grants permission to obtain proactive defense statistics.                                                            | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |

| Action                                             | Description                                                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:overview:getOverviewProtectionStatusStatistics | Grants permission to query the protection status of the current cloud load.                         | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewQuotaStatistics            | Grants permission to obtain server security statistics.                                             | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewRiskLists                  | Grants permission to query the risk list.                                                           | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewRiskManagementStatistics   | Grants permission to obtain risk management information, including risk trends and type statistics. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewRiskScore                  | Grants permission to query risk scores.                                                             | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewRiskStatistics             | Grants permission to query risk statistics, security risks, security alarms, and proactive defense. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:getOverviewTrialsStatistics           | Grants permission to try server risk statistics.                                                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |

| Action                                               | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|------------------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:antiransomware:getRansomwareBackupInfoByBackupId | Grants permission to query specified backup information.       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:getRansomwareHSSBackupPolicyInfo  | Grants permission to query backup policy information.          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:getRansomwareBackupStatistics     | Grants permission to query backup statistics.                  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:getRansomwareProtectionStatistics | Grants permission to query protection statistics.              | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:getRansomwareVaultInfo            | Grants permission to query backup vault information.           | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:rasp:getRaspPolicyDetail                         | Grants permission to query protection policy details.          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:list</li> </ul>           |
| hss:rasp:getRaspProtectStatistics                    | Grants permission to obtain protection data statistics.        | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:list</li> </ul>           |
| hss:wtp:getRaspSwitchStatus                          | Grants permission to query whether the dynamic WTP is enabled. | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpHosts:list</li> </ul>       |

| Action                                         | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|------------------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:securitycheck:getSecurityCheckConfig       | Grants permission to query security check schedules.                        | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:list</li> </ul> |
| hss:securitycheck:getSecurityCheckHostReport   | Grants permission to query the security check report of a specified server. | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:list</li> </ul> |
| hss:securitycheck:getSecurityCheckOverview     | Grants permission to query the security check overview.                     | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:list</li> </ul> |
| hss:securitycheck:getSecurityCheckStatistics   | Grants permission to query security check statistics.                       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:list</li> </ul> |
| hss:safetyReport:getSecurityReport             | Grants permission to query the content of the security report.              | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:list</li> </ul>  |
| hss:safetyReport:getSecurityReportSubscription | Grants permission to query the content of a report subscription.            | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:list</li> </ul>  |

| Action                                       | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|----------------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:wtp:getTimingOffStatusInfo               | Grants permission to query whether a protection configuration is in the scheduled disabling list. | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpScheduledProtections:get</li> </ul> |
| hss:wtp:getWtpDashboardProtectStatistics     | Grants permission to query protection statistics.                                                 | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDashboard:get</li> </ul>            |
| hss:wtp:getWtpDirectory                      | Grants permission to query the Tomcat bin directory for dynamic WTP.                              | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectories:list</li> </ul>         |
| hss:wtp:getWtpDirectoryMonitorOnlyStatus     | Grants permission to query the status of the monitoring-only switch.                              | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectories:list</li> </ul>         |
| hss:wtp:getWtpPrivilegedProcessesChildStatus | Grants permission to display the trust status of privileged subprocesses.                         | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpPrivilegedProcesses:list</li> </ul> |
| hss:wtp:getWtpRemoteBackupHostInfo           | Grants permission to query information about the remote backup server.                            | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpProtectMode:get</li> </ul>          |

| Action                               | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                  |
|--------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------|
| hss:setting:listAgentVersion         | Grants permission to query agent versions.                      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:installAgent:get</li> </ul> |
| hss:container:listContainerNodes     | Grants permission to query the container node list.             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul>  |
| hss:keyfile:listFileEvents           | Grants permission to obtain the list of changed files.          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:keyfiles:list</li> </ul>    |
| hss:keyfile:listFileHostEventDetails | Grants permission to obtain details about a server change file. | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:keyfiles:list</li> </ul>    |
| hss:keyfile:listFileHosts            | Grants permission to obtain the ECS change list.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:keyfiles:list</li> </ul>    |
| hss:host:listHostGroups              | Grants permission to query the server group list.               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:get</li> </ul>    |
| hss:setting:listLoginCommonIp        | Grants permission to query common login IP addresses.           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:commonIPs:list</li> </ul>   |

| Action                              | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                      |
|-------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------------|
| hss:setting:listLoginCommonLocation | Grants permission to query common login locations.                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:commonLocations:list</li> </ul> |
| hss:setting:listLoginWhitelist      | Grants permission to query the login IP address whitelist.             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:whitelists:list</li> </ul>      |
| hss:policy:listPolicyGroup          | Grants permission to query the policy group list.                      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:get</li> </ul>           |
| hss:asset:listPortHost              | Grants permission to query asset fingerprints - port - server list.    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ports:list</li> </ul>           |
| hss:asset:listProcessesHost         | Grants permission to query asset fingerprints - process - server list. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:processes:list</li> </ul>       |
| hss:ars:listPWLEvent                | Grants permission to query process whitelist events.                   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>             |
| hss:ars:listPwlPolicy               | Grants permission to query the process whitelist policy list.          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>             |



| Action                                                    | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|-----------------------------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:ars:listPwlPolicyHost                                 | Grants permission to query the servers associated with a process whitelist policy. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>            |
| hss:ars:listPwlPolicyProcess                              | Grants permission to query the process whitelist policy identification processes.  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>            |
| hss:antiransomware:listRansomwareBackupByHostId           | Grants permission to query the vulnerability list.                                 | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:listRansomwareOperationLogsByVaultName | Grants permission to query the backup and restoration task list.                   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:listRansomwareProtectionOptionalServer | Grants permission to query the servers under ransomware protection.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:listRansomwareProtectionPolicy         | Grants permission to query protection policies.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |

| Action                                               | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|------------------------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:antiransomware:listRansomwareProtectionServer    | Grants permission to query servers protected against ransomware.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:rasp:listRaspCheckFeatureRule                    | Grants permission to query detection rules.                                         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:list</li> </ul>           |
| hss:rasp:listRaspEvents                              | Grants permission to query application protection events.                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:list</li> </ul>           |
| hss:rasp:listRaspPolicies                            | Grants permission to query protection policies.                                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:list</li> </ul>           |
| hss:rasp:listRaspProtectionServers                   | Grants permission to query protected servers.                                       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:list</li> </ul>           |
| hss:securitycheck:listSecurityCheckHostReportHistory | Grants permission to query historical security check reports of a specified server. | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:list</li> </ul>  |
| hss:securitycheck:listSecurityCheckHostResult        | Grants permission to query the security check results of servers.                   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:list</li> </ul>  |

| Action                                           | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|--------------------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:safetyReport:listSecurityReport              | Grants permission to query the list on the report overview page.              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:list</li> </ul>           |
| hss:safetyReport:listSecurityReportHistoryPeriod | Grants permission to query the statistical period list of historical reports. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:list</li> </ul>           |
| hss:safetyReport:listSecurityReportSendingRecord | Grants permission to query report sending records.                            | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:list</li> </ul>           |
| hss:wtp:listTimingOffConfigInfo                  | Grants permission to query the scheduled disabling list.                      | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpScheduledProtections:get</li> </ul> |
| hss:setting:listTwoFactorLoginHost               | Grants permission to query the list of servers with 2FA enabled.              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:twofactorAuth:list</li> </ul>          |
| hss:wtp:listWtpBackupHostsInfo                   | Grants permission to query the remote backup server.                          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpBackup:get</li> </ul>               |
| hss:wtp:listWtpHostProtectDirInfo                | Grants permission to query protected directories.                             | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectories:list</li> </ul>         |

| Action                                    | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|-------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:wtp:listWtpHostProtectHistoryInfo     | Grants permission to query the static WTP status of the server.      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpReports:list</li> </ul>             |
| hss:wtp:listWtpHostRaspProtectHistoryInfo | Grants permission to query the dynamic WTP status of the server.     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpReports:list</li> </ul>             |
| hss:wtp:listWtpPrivilegedProcessesInfo    | Grants permission to query privileged process configurations.        | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpPrivilegedProcesses:list</li> </ul> |
| hss:wtp:listWtpProtectHost                | Grants permission to query the protection list.                      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpHosts:list</li> </ul>               |
| hss:setting:modifyLoginCommonIp           | Grants permission to add, edit, or delete common login IP addresses. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:commonIPs:set</li> </ul>               |
| hss:setting:modifyLoginCommonLocation     | Grants permission to add, edit, or delete common login locations.    | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:commonLocations:set</li> </ul>         |

| Action                                              | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|-----------------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:setting:modifyLoginWhitelist                    | Grants permission to add, edit, or delete the login IP address whitelist. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:whitelists:set</li> </ul>     |
| hss:ars:operatePWLEvent                             | Grants permission to handle events.                                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>            |
| hss:ars:relearnPWLPolicy                            | Grants permission to relearn whitelist policies.                          | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>            |
| hss:overview:resetOverviewRiskScore                 | Grants permission to reset risk scores and perform health checks again.   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:set</li> </ul>       |
| hss:antiransomware:restoreRansomwareDuplicationInfo | Grants permission to back up and restore data.                            | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul> |
| hss:safetyReport:sendSecurityReport                 | Grants permission to send security reports.                               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:set</li> </ul>   |
| hss:setting:setAlarmConfig                          | Grants permission to configure prompt information.                        | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:alertConfig:get</li> </ul>    |

| Action                                       | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|----------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:setting:setMalwareReminders              | Grants permission to configure prompt information.                         | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:automaticKillMp:set</li> </ul>         |
| hss:wtp:setRemoteWtpBackupInfo               | Grants permission to enable or disable remote backup.                      | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpBackup:set</li> </ul>               |
| hss:wtp:setTimingOffSwitchInfo               | Grants permission to set the status of the scheduled protection disabling. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpScheduledProtections:set</li> </ul> |
| hss:setting:setTwoFactorLoginConfig          | Grants permission to configure 2FA login.                                  | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:twofactorAuth:set</li> </ul>           |
| hss:wtp:setWtpDirectoryMonitorOnlyStatus     | Grants permission to configure the monitoring-only switch.                 | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectories:set</li> </ul>          |
| hss:wtp:setWtpPrivilegedProcessesChildStatus | Grants permission to set the trust status of privileged subprocesses.      | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpPrivilegedProcesses:list</li> </ul> |
| hss:wtp:setWtpProtectionStatusInfo           | Grants permission to enable or disable WTP.                                | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpProtect:switch</li> </ul>           |

| Action                                             | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:wdp:setWtpProtectSwitch                        | Grants permission to enable or disable dynamic WTP.                                             | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wdpProtect:switch</li> </ul>           |
| hss:wdp:setWtpScheduledProtectionDateOffConfigInfo | Grants permission to configure the frequency and period for automatically disabling protection. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wdpScheduledProtections:set</li> </ul> |
| hss:securitycheck:startManualSecurityCheck         | Grants permission to start a manual health check.                                               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:set</li> </ul>           |
| hss:antiransomware:startRansomwareBackupSingle     | Grants permission to enable the backup function for a single server.                            | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>          |
| hss:antiransomware:startRansomwareProtection       | Grants permission to enable ransomware protection.                                              | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>          |
| hss:antiransomware:startRansomwareProtectionSingle | Grants permission to enable ransomware protection for a single server.                          | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>          |
| hss:securitycheck:stopManualSecurityCheck          | Grants permission to cancel a manual health check.                                              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:set</li> </ul>           |

| Action                                        | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|-----------------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:antiransomware:stopRansomwareProtection   | Grants permission to disable ransomware protection.               | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul> |
| hss:container:switchContainerProtectionStatus | Grants permission to switch the protection status.                | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:set</li> </ul>     |
| hss:ars:switchPWLPolicyHost                   | Grants permission to enable or disable a server whitelist policy. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>            |
| hss:rasp:switchRasp                           | Grants permission to enable or disable application protection.    | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:set</li> </ul>           |
| hss:safetyReport:switchSecurityReportStatus   | Grants permission to enable or disable security reports.          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:safetyReport:set</li> </ul>   |
| hss:wtp:switchWtpHostProtectDirInfo           | Grants permission to enable or disable directory protection.      | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectories:set</li> </ul> |
| hss:host:uninstallAgents                      | Grants permission to uninstall the agent.                         | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:agent:uninstall</li> </ul>    |



| Action                                              | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|-----------------------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| hss:setting:updateAlarmConfig                       | Grants permission to configure alarm configurations.                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:alertConfig:set</li> </ul>             |
| hss:antiransomware:updateRansomwareBackupPolicyInfo | Grants permission to modify backup policies.                                     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>          |
| hss:antiransomware:updateRansomwareProtectionPolicy | Grants permission to modify protection policies.                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>          |
| hss:rasp:updateRaspPolicy                           | Grants permission to modify protection policies.                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:rasp:set</li> </ul>                    |
| hss:securitycheck:updateSecurityCheckConfig         | Grants permission to modify security check schedules.                            | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:securitycheck:set</li> </ul>           |
| hss:wtp:updateTimingOffConfigInfo                   | Grants permission to modify the configuration of scheduled protection disabling. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpScheduledProtections:set</li> </ul> |
| hss:wtp:updateWtpBackupHostInfo                     | Grants permission to add or modify a remote backup server.                       | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpBackup:set</li> </ul>               |

| Action                                 | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                          |
|----------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------------|
| hss:wtp:updateWtpDirectoryInfo         | Grants permission to modify the Tomcat bin directory of dynamic WTP.                    | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectory:set</li> </ul>         |
| hss:wtp:updateWtpHostProtectDirInfo    | Grants permission to modify protected directories.                                      | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpDirectory:set</li> </ul>         |
| hss:wtp:updateWtpPrivilegedProcessInfo | Grants permission to modify privileged processes.                                       | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:wtpPrivilegedProcess:set</li> </ul> |
| hss:asset:addValuesLevel               | Grants permission to configure asset management - server management - asset importance. | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:set</li> </ul>               |
| hss:asset:batchModifyPortStatus        | Grants permission to change port status.                                                | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ports:operate</li> </ul>            |
| hss:asset:deleteToolConditionHistory   | Grants permission to clear the search records of tools (operation tool).                | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:set</li> </ul>               |

| Action                             | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:executeTool              | Grants permission to perform search with tools (operation tools).                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:set</li> </ul>  |
| hss:asset:getAccountTop            | Grants permission to obtain asset management - overview - top accounts.                       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getAgentStatisticsStatus | Grants permission to obtain asset management - overview - asset status - server agent status. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getAssetStatistic        | Grants permission to obtain asset statistics, including accounts, ports, and processes.       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getAssetType             | Grants permission to obtain asset management - overview - asset status - asset distribution.  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                                 | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|----------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:getAutoLaunchTop             | Grants permission to obtain asset management - overview - top auto-started items.                     | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getCommonPort                | Grants permission to display details about a port.                                                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getContainerProtectionStatus | Grants permission to obtain asset management - overview - asset status - container protection status. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getCoreConfFileTop           | Grants permission to obtain asset management - overview - top key configurations .                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getEnvironmentTop            | Grants permission to obtain asset management - overview - top environment variables.                  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                                    | Description                                                                                                      | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:getHostAssetManualCollectStatus | Grants permission to obtain the status of the API for immediately collecting the asset fingerprints of a server. | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getHostProtectionStatus         | Grants permission to obtain asset management - overview - asset status - agent status.                           | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getJarPackageTop                | Grants permission to obtain asset management - overview - top JAR packages.                                      | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getKernelModuleTop              | Grants permission to obtain asset management - overview - top kernel modules.                                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getOSStatisticsInfo             | Grants permission to obtain asset management - overview - asset status - OS statistics.                          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                           | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:getProcessTop          | Grants permission to obtain asset management - overview - top processes.                              | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getPortTop             | Grants permission to obtain asset management - overview - top ports.                                  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getQuotaStatisticsInfo | Grants permission to obtain asset management - overview - asset status - protection quota statistics. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getSoftwareTop         | Grants permission to obtain asset management - overview - top software.                               | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getWebAppAndServiceTop | Grants permission to obtain asset management - overview - top web apps and services.                  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:getWebAppTop           | Grants permission to obtain asset management - overview - top web applications.                       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                           | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                |
|----------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------|
| hss:asset:getWebFrameworkTop     | Grants permission to obtain asset management - overview - top web frameworks.              | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>    |
| hss:asset:getWebServiceTop       | Grants permission to obtain asset management - overview - top web services.                | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>    |
| hss:asset:getWebSiteTop          | Grants permission to obtain asset management - overview - top websites.                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>    |
| hss:asset:listAppChangeHistories | Grants permission to obtain asset fingerprints - software information - operation history. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:softwares:list</li> </ul> |
| hss:asset:listApps               | Grants permission to obtain asset fingerprints of a single server - software.              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:softwares:list</li> </ul> |
| hss:asset:listAppStatistics      | Grants permission to obtain asset fingerprints - software information.                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:softwares:list</li> </ul> |

| Action                                  | Description                                                                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:listAutoLaunchChangeHistories | Grants permission to obtain asset fingerprints - auto-started items - change history.                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listAutoLaunches              | Grants permission to obtain asset fingerprints of a server - auto-started items.                                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:launch:list</li> </ul> |
| hss:asset:listAutoLaunchStatistics      | Grants permission to obtain asset fingerprints - auto-started items.                                            | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:launch:list</li> </ul> |
| hss:asset:listCoreConfFileHostInfo      | Grants permission to obtain asset management - asset fingerprints - the server list of key configuration files. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listCoreConfFileInfo          | Grants permission to obtain asset management - server management - fingerprint type - key configurations.       | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |



| Action                               | Description                                                                                                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:listCoreConfFileStatistics | Grants permission to obtain asset management<br>- asset fingerprints - key configuration file navigation tree on the left.                                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listEnvironmentHostInfo    | Grants permission to obtain asset management<br>- asset fingerprints - the server list of key environment variables (on the right of asset fingerprints). | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listEnvironmentInfo        | Grants permission to obtain asset management<br>- server management<br>- fingerprint type - environment variables.                                        | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                              | Description                                                                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:listEnvironmentStatistics | Grants permission to obtain asset management - asset fingerprints - environment variable file navigation tree on the left. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listJarPackageHostInfo    | Grants permission to obtain asset management - asset fingerprints - the server list of JAR packages.                       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listJarPackageInfo        | Grants permission to obtain asset management - server management - fingerprint type - JAR packages.                        | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listJarPackageStatistics  | Grants permission to obtain asset management - asset fingerprints - JAR package navigation tree on the left.               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                               | Description                                                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:listKernelModuleHostInfo   | Grants permission to obtain asset management - asset fingerprints - the server list of kernel modules.         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listKernelModuleInfo       | Grants permission to obtain asset management - server management - fingerprint type - kernel modules.          | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listKernelModuleStatistics | Grants permission to obtain asset management - asset fingerprints - kernel module navigation tree on the left. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listPorts                  | Grants permission to obtain single-server asset fingerprint (open port information).                           | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ports:list</li> </ul>  |
| hss:asset:listPortStatistics         | Grants permission to obtain asset fingerprints (open port information).                                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ports:list</li> </ul>  |

| Action                             | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                |
|------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------|
| hss:asset:listProcesses            | Grants permission to obtain the process list.                              | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:processes:list</li> </ul> |
| hss:asset:listProcessStatistics    | Grants permission to obtain asset fingerprints (process information).      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:processes:list</li> </ul> |
| hss:asset:listResult               | Grants permission to obtain execution results (operation tools).           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>    |
| hss:asset:listTool                 | Grants permission to obtain the tool list (operation tools).               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>    |
| hss:asset:listToolConditionHistory | Grants permission to obtain the search records of tools (operation tools). | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>    |
| hss:asset:listUserChangeHistories  | Grants permission to obtain the account change history.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:accounts:list</li> </ul>  |
| hss:asset:listUserGroup            | Grants permission to obtain the user group list.                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>    |

| Action                                   | Description                                                                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:asset:listUsers                      | Grants permission to obtain the account list of assets.                                                              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:accounts:list</li> </ul> |
| hss:asset:listUserStatistics             | Grants permission to obtain asset fingerprints - software information.                                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:accounts:list</li> </ul> |
| hss:asset:listWebAppAndServices          | Grants permission to obtain asset management - asset fingerprints - web app and service assets on the right.         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>   |
| hss:asset:listWebAppAndServiceStatistics | Grants permission to obtain asset management - asset fingerprints - web app and service navigation tree on the left. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>   |
| hss:asset:listWebAppHostInfo             | Grants permission to obtain asset management - asset fingerprints - the server list of web applications.             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>   |

| Action                             | Description                                                                                                      | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:listWebAppInfo           | Grants permission to obtain asset management - server management - fingerprint type - web applications.          | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listWebAppStatistics     | Grants permission to obtain asset management - asset fingerprints - web application navigation tree on the left. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listWebFrameworkHostInfo | Grants permission to obtain asset management - asset fingerprints - the server list of web frameworks.           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listWebFrameworkInfo     | Grants permission to obtain asset management - server management - fingerprint type - web frameworks.            | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                               | Description                                                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:asset:listWebFrameworkStatistics | Grants permission to obtain asset management - asset fingerprints - web framework navigation tree on the left. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listWebServiceHostInfo     | Grants permission to obtain asset management - asset fingerprints - the server list of web servers.            | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listWebServiceInfo         | Grants permission to obtain asset management - server management - fingerprint type - web services.            | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |
| hss:asset:listWebServiceStatistics   | Grants permission to obtain asset management - asset fingerprints - web services navigation tree on the left.  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul> |

| Action                                   | Description                                                                                              | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|------------------------------------------|----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:asset:listWebSiteHostInfo            | Grants permission to obtain asset management - asset fingerprints - the server list of websites.         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>   |
| hss:asset:listWebSiteInfo                | Grants permission to obtain asset management - server management - fingerprint type - websites.          | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>   |
| hss:asset:listWebSiteStatistics          | Grants permission to obtain asset management - asset fingerprints - website navigation tree on the left. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:list</li> </ul>   |
| hss:asset:runHostAssetManualCollect      | Grants permission to immediately collect the asset fingerprints of a server.                             | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:assets:set</li> </ul>    |
| hss:baseline:addSecurityCheckPolicyGroup | Grants permission to create a configuration detection policy.                                            | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:set</li> </ul> |



| Action                                      | Description                                                                                 | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                       |
|---------------------------------------------|---------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------|
| hss:baseline:changeCheckRuleState           | Grants permission to ignore, unignore, repair, and verify failed configuration check items. | Write        | baseline *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:configDetects:operate</li> </ul> |
| hss:baseline:deleteSecurityCheckPolicyGroup | Grants permission to delete a specified configuration detection policy.                     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:set</li> </ul>         |
| hss:baseline:exportSecurityCheckReport      | Grants permission to export the configuration detection report.                             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:configDetects:list</li> </ul>    |
| hss:baseline:getBaselineOverview            | Grants permission to query baseline check statistics.                                       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>        |
| hss:baseline:getBaselineScanStatus          | Grants permission to query the progress of a baseline check task.                           | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>        |

| Action                                            | Description                                                                                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:baseline:getBaselineStatistic                 | Grants permission to query baseline check statistics, including weak passwords, password complexity, and configuration detection. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>     |
| hss:baseline:getCheckRuleDetail                   | Grants permission to query the check report of a configuration check item.                                                        | Read         | baseline *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:configDetects:list</li> </ul> |
| hss:baseline:getCheckRuleFixFailDetail            | Grants permission to query the cause of the check item repair failure.                                                            | Read         | baseline *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>     |
| hss:baseline:getDefaultSecurityCheckPolicy        | Grants permission to query the default baseline of a configuration detection policy.                                              | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>     |
| hss:baseline:getDefaultSecurityCheckPolicyDetails | Grants permission to query detailed baseline check items.                                                                         | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>     |

| Action                                | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                         |
|---------------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------------------|
| hss:baseline:getRiskConfigDetail      | Grants permission to query the check result of a specified security configuration item.    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:configDetects:list</li> </ul>      |
| hss:baseline:listCheckRuleHost        | Grants permission to query servers covered by a configuration check item.                  | List         | baseline *                  | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>          |
| hss:baseline:listPasswordComplexity   | Grants permission to query the password complexity policy check report.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:complexityPolicies:list</li> </ul> |
| hss:baseline:listRiskConfigCheckRules | Grants permission to query the check item list of a specified security configuration item. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:configDetects:list</li> </ul>      |
| hss:baseline:listRiskConfigHosts      | Grants permission to query servers affected by a specified security configuration item.    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:riskConfigHosts:list</li> </ul>    |

| Action                                      | Description                                                                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:baseline:listRiskConfigs                | Grants permission to query the server security configuration check result list of a tenant.                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:configDetects:list</li> </ul> |
| hss:baseline:listSecurityCheckPolicyGroup   | Grants permission to query the list of configuration detection policy groups.                                             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:list</li> </ul>     |
| hss:baseline:listWeakPasswordUsers          | Grants permission to query the weak password detection results.                                                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:weakPasswords:list</li> </ul> |
| hss:baseline:runBaselineDetect              | Grants permission to perform manual detection for weak passwords and configurations on the servers specified in a policy. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:set</li> </ul>      |
| hss:baseline:updateSecurityCheckPolicyGroup | Grants permission to modify a specified configuration detection policy.                                                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:baselines:set</li> </ul>      |

| Action                           | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                           |
|----------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------|
| hss:event:addLoginWhiteList      | Grants permission to add a login whitelist.                               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul> |
| hss:event:batchChangeEvent       | Grants permission to handle alarm events in batches.                      | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul> |
| hss:event:changeEvent            | Grants permission to handle alarm events.                                 | Write        | event *                     | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul> |
| hss:event:changeIsolatedFile     | Grants permission to restore isolated files.                              | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul> |
| hss:event:exportAlarmWhiteList   | Grants permission to export the alarm whitelist.                          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
| hss:event:exportEmergency        | Grants permission to export emergency malware.                            | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul> |
| hss:event:getEmergencyStatistics | Grants permission to obtain emergency event statistics.                   | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
| hss:event:getEventAttackTag      | Grants permission to query the list of attack ID distribution statistics. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |

| Action                            | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|-----------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:event:getEventSeverity        | Grants permission to query the list of threat level statistics.       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>          |
| hss:event:getEventStatistics      | Grants permission to query alarm event statistics.                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>          |
| hss:event:getMalwareInfo          | Grants permission to obtain the list of details about sudden malware. | Read         | event *                     | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>          |
| hss:event:handleMalwareEvent      | Grants permission to handle malware.                                  | Write        | event *                     | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>          |
| hss:event:importAlarmWhiteList    | Grants permission to import an alarm whitelist.                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>          |
| hss:event:isolateOperateEmergency | Grants permission to enable or disable the isolation box.             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>          |
| hss:event:listAlarmWhiteList      | Grants permission to query the alarm whitelist.                       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>          |
| hss:event:listBlockedIp           | Grants permission to query the list of blocked IP addresses.          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:accountCracks:list</li> </ul> |

| Action                         | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                           |
|--------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------|
| hss:event:listEventOperates    | Grants permission to query the handling types supported by events.        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
| hss:event:listEventTopRisk     | Grants permission to query the list of top 10 event type statistics.      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
| hss:event:listEventType        | Grants permission to query the list of event type statistics.             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
| hss:event:listFilesIsolateList | Grants permission to obtain the list of files isolated by sudden malware. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
| hss:event:listIsolatedFile     | Grants permission to query the isolated file list.                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
| hss:event:listLoginWhiteList   | Grants permission to query the login whitelist.                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |

| Action                           | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|----------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:event:listMalware            | Grants permission to obtain the list of unexpected malicious program events. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>     |
| hss:event:listSecurityEvents     | Grants permission to query the intrusion event list.                         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>     |
| hss:event:recoverIsolateFile     | Grants permission to restore the file isolation box.                         | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>     |
| hss:event:removeAlarmWhitelist   | Grants permission to delete an alarm whitelist.                              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>     |
| hss:event:removeLoginWhitelist   | Grants permission to delete a login whitelist.                               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>     |
| hss:host:associateHostAssetValue | Grants permission to associate asset importance.                             | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:set</li> </ul>     |
| hss:host:associateHostsGroup     | Grants permission to allocate servers to a server group.                     | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:set</li> </ul> |
| hss:host:batchInstallAgent       | Grants permission to install agents in batches.                              | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:set</li> </ul>     |



| Action                           | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|----------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:host:changeHostsGroup        | Grants permission to edit a server group.                                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:set</li> </ul> |
| hss:host:deleteHostsGroup        | Grants permission to delete a server group.                                           | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:set</li> </ul> |
| hss:host:getHostsStatistics      | Grants permission to collect server statistics.                                       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>    |
| hss:host:listFirewallStatus      | Grants permission to query the firewall status of a server.                           | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>    |
| hss:host:listHostGroupAssetValue | Grants permission to query the list of servers in a server group by asset importance. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>    |
| hss:host:listHostsRisk           | Grants permission to obtain ECS risk status.                                          | Read         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>    |
| hss:host:listHostStatus          | Grants permission to query the list of protected servers.                             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>    |
| hss:host:listHostsUpgrade        | Grants permission to obtain the agent upgrade status of a server.                     | Read         | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>    |
|                                  |                                                                                       |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                     |

| Action                            | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|-----------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:host:manualCheckVul           | Grants permission to manually detect vulnerabilities.                      | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:manualDetect</li> </ul>  |
| hss:host:switchFirewallStatus     | Grants permission to modify the firewall authorization status.             | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:switchVersion</li> </ul> |
| hss:host:switchHostsProtectStatus | Grants permission to switch the protection status.                         | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:switchVersion</li> </ul> |
| hss:host:upgradeAgent             | Grants permission to upgrade the agent from 1.0 to 2.0.                    | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:hosts:switchVersion</li> </ul> |
|                                   |                                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                           |
| hss:host:upgradeAgents            | Grants permission to upgrade the agent.                                    | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:set</li> </ul>           |
| hss:image:batchScanLocalImage     | Grants permission to perform local image scanning.                         | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>          |
| hss:image:batchScanPrivateImage   | Grants permission to scan images in private image repositories in batches. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>          |
| hss:image:getImageFilesStat       | Grants permission to query image file statistics.                          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>         |

| Action                              | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                              |
|-------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------|
| hss:image:getImageLocalVulOverview  | Grants permission to query local vulnerabilities.                                                     | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:getImageVulOverview       | Grants permission to query repository vulnerabilities.                                                | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listCfgCheckAffectedImage | Grants permission to query the list of images affected by a tenant image that failed baseline checks. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listGlobalCfgCheck        | Grants permission to query container image baseline inspection results.                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listGlobalMalware         | Grants permission to query the list of malicious tenant files.                                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listGlobalVul             | Grants permission to query vulnerability details about a tenant image.                                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |

| Action                       | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                              |
|------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------|
| hss:image:listImageApps      | Grants permission to query the image software list.                          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageAppVul    | Grants permission to query the software vulnerability list.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageCfgCheck  | Grants permission to query configuration baseline check results of an image. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageFiles     | Grants permission to query the list of image files that have no owners.      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageLocal     | Grants permission to query the local image list.                             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageMalware   | Grants permission to query the list of malicious image files.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageNamespace | Grants permission to query the namespace of an image.                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |

| Action                             | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                              |
|------------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------|
| hss:image:listImageRepository      | Grants permission to query the list of images in a private image repository.               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageVul             | Grants permission to query image vulnerability details.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listInstanceImageVul     | Grants permission to query vulnerability details about enterprise images.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listLocalImageApp        | Grants permission to query the local software image list.                                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listLocalImageAppVuls    | Grants permission to query the vulnerability list of a piece of software in a local image. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listLocalImageContainers | Grants permission to query the container information about a local image.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |

| Action                               | Description                                                                                             | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                              |
|--------------------------------------|---------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------|
| hss:image:listLocalImageHosts        | Grants permission to query the server information about a local image.                                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listLocalImageMalware      | Grants permission to query malicious file information about local images.                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listLocalImageVulns        | Grants permission to query vulnerability information about a local image.                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listLocalVulRepoImage      | Grants permission to query details about images and containers affected by local image vulnerabilities. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listPrivateImageRepository | Grants permission to query the list of images in a private image repository.                            | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |

| Action                              | Description                                                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                              |
|-------------------------------------|------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------|
| hss:image:listSharedImageRepository | Grants permission to query the list of images in the shared image repository.                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listVulCve                | Grants permission to query CVE details about a vulnerability.                                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listVulRepoImage          | Grants permission to query details about images in the image repository affected by a vulnerability. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:runImageScan              | Grants permission to scan images.                                                                    | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: set</li> </ul>  |
| hss:image:runImageSynchronizeTask   | Grants permission to synchronize the free image list from SWR.                                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: set</li> </ul>  |
| hss:image:runSwrImageScan           | Grants permission to update and scan SWR images and to access SWR.                                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: set</li> </ul>  |

| Action                               | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                            |
|--------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------|
| hss:image:sharedImageSynchronization | Grants permission to update images shared from SWR.                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul> |
| hss:policy:addPolicyGroup            | Grants permission to copy server policy groups.                           | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:set</li> </ul> |
| hss:policy:associatePolicyGroup      | Grants permission to deploy a policy.                                     | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:set</li> </ul> |
|                                      |                                                                           |              | host *                      | <a href="#">g:EnterpriseProjectId</a> |                                                                  |
| hss:policy:changePolicyDetail        | Grants permission to modify a policy.                                     | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:set</li> </ul> |
| hss:policy:changePolicyGroup         | Grants permission to modify policy groups.                                | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:set</li> </ul> |
| hss:policy:deletePolicyGroup         | Grants permission to delete policy groups.                                | Write        | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:set</li> </ul> |
| hss:policy:getPolicyDetail           | Grants permission to query details about a specified policy.              | Read         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:get</li> </ul> |
| hss:policy:listPolicyGroupDetail     | Grants permission to query the policy information list of a policy group. | List         | policy *                    | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:policy:get</li> </ul> |



| Action                              | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias            |
|-------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------|
| hss:quota:addResourceInstanceTag    | Grants permission to add tags to a resource.                         | Tagging      | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • hss:quotas:set |
| hss:quota:batchCreateTags           | Grants permission to create tags in batches.                         | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • hss:quotas:set |
| hss:quota:batchDeleteTags           | Grants permission to delete tags in batches.                         | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • hss:quotas:set |
| hss:quota:cancelHostsQuota          | Grants permission to unbind quotas.                                  | Write        | -                           | -                                                                                                                                     | • hss:quotas:set |
| hss:quota:changeTmsResourceTagInfo  | Grants permission to add or delete resource tags in batches.         | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • hss:quotas:set |
| hss:quota:countResourceInstances    | Grants permission to query the number of purchased resources by tag. | List         | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • hss:quotas:set |
| hss:quota:dealOrder                 | Grants permission to purchase quotas.                                | Write        | -                           | -                                                                                                                                     | • hss:quotas:set |
| hss:quota:deleteResourceInstanceTag | Grants permission to delete tags from a resource.                    | Tagging      | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • hss:quotas:set |

| Action                                 | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias                                                               |
|----------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| hss:quota:filterResourceInstanceList   | Grants permission to search for purchased resources by tag.      | List         | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>• hss:quotas: set</li> </ul> |
| hss:quota:getResourceInstanceTag       | Grants permission to query tags of a resource.                   | Read         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• hss:quotas: get</li> </ul> |
| hss:quota:getResourceQuotas            | Grants permission to query quota information.                    | Read         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• hss:quotas: get</li> </ul> |
| hss:quota:getTmsResourceTagsInfo       | Grants permission to query resource tags.                        | Read         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• hss:quotas: get</li> </ul> |
| hss:quota:listProjectTags              | Grants permission to query all used tags in the current project. | List         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• hss:quotas: get</li> </ul> |
| hss:quota:listQuotasDetail             | Grants permission to query quota details.                        | List         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• hss:quotas: get</li> </ul> |
| hss:quota:listResourceIds              | Grants permission to query quota IDs in batches.                 | List         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• hss:quotas: get</li> </ul> |
| hss:quota:listTmsResourceInstancesInfo | Grants permission to query resource instances.                   | List         | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>• hss:quotas: get</li> </ul> |

| Action                                           | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                            |
|--------------------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------|
| hss:quota:upgradeOrder                           | Grants permission to change specifications.                                               | Write        | -                           | -                                     | <ul style="list-style-type: none"> <li>hss:quotas:set</li> </ul> |
| hss:vulnerability:changeVulStatus                | Grants permission to modify the status of a vulnerability.                                | Write        | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>   |
| hss:vulnerability:exportEmergencyVulnerabilities | Grants permission to export emergency vulnerabilities.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>   |
| hss:vulnerability:exportVulList                  | Grants permission to export information about vulnerabilities and their affected servers. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>  |
| hss:vulnerability:getCmsVulDetail                | Grants permission to query basic information about the Web-CMS vulnerabilities.           | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>  |
| hss:vulnerability:getEmergencySummary            | Grants permission to query the event overview.                                            | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>  |
| hss:vulnerability:getEmergencyVulDetail          | Grants permission to query vulnerability details in events.                               | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>  |

| Action                                | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                        |
|---------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------|
| hss:vulnerability:getLinuxVulDetail   | Grants permission to query basic information about Linux vulnerabilities.     | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:vulnerability:getVulCheckStatus   | Grants permission to query the status of server vulnerability scanning.       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:manualDetectStatus:get</li> </ul> |
| hss:vulnerability:getVulSummary       | Grants permission to query vulnerability statistics.                          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:vulnerability:getWindowsVulDetail | Grants permission to query basic information about Windows vulnerabilities.   | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:vulnerability:getWindowsVulNum    | Grants permission to query the number of Windows vulnerabilities on a server. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:vulnerability:listEmergencyVul    | Grants permission to query vulnerabilities in events.                         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |

| Action                                      | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                         | Alias           |
|---------------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------|
| hss:vulnerability:listHostVuls              | Grants permission to query vulnerability information about a single server. | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | • hss:vuls:list |
| hss:vulnerability:listHostVulSummary        | Grants permission to query server statistics and top 5 risky servers.       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:vuls:list |
| hss:vulnerability:listTopVulSummary         | Grants permission to query top 5 vulnerabilities.                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:vuls:list |
| hss:vulnerability:listVulHosts              | Grants permission to query ECSs affected by a specific vulnerability.       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:vuls:list |
| hss:vulnerability:listVulnerabilities       | Grants permission to query the vulnerability list.                          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:vuls:list |
| hss:vulnerability:listVulRepairFailedDetail | Grants permission to query information about vulnerability fixing failures. | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | • hss:vuls:list |
| hss:vulnerability:listVulTypeSummary        | Grants permission to query vulnerability type distribution.                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:vuls:list |

| Action                             | Description                                             | Access Level          | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|------------------------------------|---------------------------------------------------------|-----------------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:vulnerability:operateEmergency | Grants permission to operate vulnerabilities in events. | Write                 | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>           |
| hss:host:getScanStatus             | Grants permission to query the manual scan status.      | Read                  | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:get</li> </ul>      |
| hss:host:setManualDetect           | Grants permission to deliver a manual scan.             | Write                 | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:manualDetect</li> </ul> |
| hss::getTrustServiceStatus         | Grants permission to get trust-service status.          | Read                  | -                           | -                                     | -                                                                        |
| hss::enableTrustService            | Grants permission to enable trust-service.              | Permission management | -                           | -                                     | -                                                                        |
| hss::validateAdmin                 | Grants permission to validate admin accounts.           | Tagging               | -                           | -                                     | -                                                                        |
| hss::listAccounts                  | Grants permission to list accounts.                     | List                  | -                           | -                                     | -                                                                        |
| hss::batchAddAccounts              | Grants permission to batch add accounts.                | Write                 | -                           | -                                     | -                                                                        |
| hss::deleteAccount                 | Grants permission to delete account by id.              | Write                 | -                           | -                                     | -                                                                        |

| Action                                           | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|--------------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss::listOrganizationTree                        | Grants permission to list organization tree.                         | List         | -                           | -                                     | -                                                                         |
| hss::listDelegatedAccounts                       | Grants permission to list organization tree.                         | List         | -                           | -                                     | -                                                                         |
| hss:antiransomware:listBackupVaults              | Grants permission to query the list of backup vaults.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:listRansomwareProtectionNodes | Grants permission to query servers protected against ransomware.     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:getBackupStatistics           | Grants permission to query backup statistics.                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:startSingleBackup             | Grants permission to enable the backup function for a single server. | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>  |
|                                                  |                                                                      |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                           |
| hss:antiransomware:getBackupPolicyInfo           | Grants permission to query single backup policy information.         | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |

| Action                               | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|--------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:hostGroup:getOutsideGroupStatus  | Grants permission to query whether creating a data center server group is supported. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:get</li> </ul> |
| hss:hostGroup:getOutsideHostGroup    | Grants permission to query offline data center server groups.                        | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:get</li> </ul> |
| hss:hostGroup:addOutsideHostGroup    | Grants permission to create an offline data center server group.                     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:set</li> </ul> |
| hss:hostGroup:changeOutsideHostGroup | Grants permission to edit an offline data center server group.                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hostGroup:set</li> </ul> |
| hss:images:listImageTag              | Grants permission to query the image tag version list.                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>   |
| hss:images:listImageSensitive        | Grants permission to query sensitive information about the image.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>   |



| Action                                | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|---------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:images:getFilePathWhiteDetail     | Grants permission to query the mirror's sensitive information file path whitelist.  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul> |
| hss:images:changeFilePathWhiteDetail  | Grants permission to modify the mirror's sensitive information file path whitelist. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>  |
| hss:images:changeSensitiveInfo        | Grants permission to handle sensitive information.                                  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>  |
| hss:event:listTopEventType            | Grants permission to query the top 5 event type statistics list.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>   |
| hss:vulnerability:getVulScanPolicy    | Grants permission to query a vulnerability scan policy.                             | Read         | -                           | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |
| hss:vulnerability:changeVulScanPolicy | Grants permission to modify a vulnerability scan policy.                            | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>    |
| hss:vulnerability:listVulWhiteList    | Grants permission to query the vulnerability whitelist.                             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |

| Action                                       | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                           |
|----------------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------|
| hss:vulnerability:getVulWhitelistDetail      | Grants permission to query vulnerability whitelist details.                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
| hss:vulnerability:changeVulWhiteList         | Grants permission to modify the vulnerability whitelist.                       | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>  |
|                                              |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:vulnerability:deleteVulWhiteList         | Grants permission to delete an item from the vulnerability whitelist.          | Write        | -                           | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>  |
| hss:vulnerability:addVulWhitelist            | Grants permission to add an item to the vulnerability whitelist.               | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>  |
|                                              |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:vulnerability:listVulWhitelistVulOptions | Grants permission to query vulnerability options when adding a whitelist item. | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
| hss:vulnerability:listVulScanTask            | Grants permission to query the vulnerability scan task list.                   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |

| Action                                     | Description                                                                                        | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                           |
|--------------------------------------------|----------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------|
| hss:vulnerability:listVulScanTaskHost      | Grants permission to query the list of servers corresponding to a vulnerability scan task.         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
| hss:vulnerability:rescanVulScanTask        | Grants permission to rescan servers in a vulnerability scan task.                                  | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>  |
|                                            |                                                                                                    |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:vulnerability:getVulScanTaskStatistics | Grants permission to query vulnerability scan task statistics.                                     | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
| hss:vulnerability:listHostVulStatistics    | Grants permission to query vulnerability management statistics.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
| hss:vulnerability:listVulHostApps          | Grants permission to query details about the software list of servers affected by vulnerabilities. | List         | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
|                                            |                                                                                                    |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:vulnerability:listVulHostProcess       | Grants permission to query details about the process list of servers affected by vulnerabilities.  | List         | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
|                                            |                                                                                                    |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |

| Action                                  | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|-----------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:vulnerability:listVulHandleHistory  | Grants permission to query historical vulnerability handling records.                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |
| hss:vulnerability:listVulHostHosts      | Grants permission to query the list of servers with vulnerabilities.                            | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |
| hss:vulnerability:listVulHostVuls       | Grants permission to query emergency fixes and unfixed vulnerabilities.                         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |
| hss:vulnerability:listVulHostHandleVuls | Grants permission to query vulnerabilities handled today and the total vulnerabilities handled. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |
| hss:image:listImageNonCompliantApp      | Grants permission to query the non-compliant software information of an image.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul> |

| Action                               | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|--------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:image:batchExportSWRVulList      | Grants permission to export vulnerabilities from an SWR image repository in batches. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>  |
| hss:image:batchExportLocalVulList    | Grants permission to export local image vulnerabilities in batches.                  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>  |
| hss:image:getExtendedWeakPassword    | Grants permission to query the user-defined weak passwords of an image.              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul> |
| hss:image:changeExtendedWeakPassword | Grants permission to modify the user-defined weak passwords of an image.             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>  |
| hss:image:listImageBasicImage        | Grants permission to query basic image information.                                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul> |
| hss:image:listImagePwdComplexity     | Grants permission to query the password complexity check report of an image.         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul> |

| Action                                  | Description                                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                              |
|-----------------------------------------|------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------|
| hss:image:listImageWeakPwdUsers         | Grants permission to query the image weak password check results of an image.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageRiskConfigs          | Grants permission to query the security configuration check results of an image.               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageRiskConfigCheckRules | Grants permission to query the check items of a specified image security configuration item.   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:getImageRiskConfigDetail      | Grants permission to query the check results of a specified image security configuration item. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:getImageCheckRuleDetail       | Grants permission to query the check reports of an image configuration check item.             | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |

| Action                              | Description                                                                                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------|
| hss:image:getImageBaselineStatistic | Grants permission to query baseline check statistics, including weak passwords, password complexity, and configuration detection. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>    |
| hss:event:addSystemUserWhitelist    | Grants permission to add users to the system user whitelist.                                                                      | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>      |
| hss:event:updateSystemUserWhitelist | Grants permission to modify the system user whitelist.                                                                            | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>      |
| hss:event:listSystemUserWhitelist   | Grants permission to query the system user whitelist.                                                                             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>      |
| hss:event:removeSystemUserWhitelist | Grants permission to remove users from the system user whitelist.                                                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>      |
| hss:container:saveClusters          | Grants permission to synchronize cluster information.                                                                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:set</li> </ul> |

| Action                            | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                 |
|-----------------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------|
| hss:container:listClusterInfo     | Grants permission to query the Kubernetes cluster list.          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listPodInfo         | Grants permission to query the basic pod information list.       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:showPodDetail       | Grants permission to query pod details.                          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listContainerInfo   | Grants permission to query the basic container information list. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:showContainerDetail | Grants permission to query container details.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listServiceInfo     | Grants permission to query the Kubernetes service list.          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:showServiceDetail   | Grants permission to query Kubernetes service details.           | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |



| Action                           | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                 |
|----------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------|
| hss:container:listEndpointInfo   | Grants permission to query the Kubernetes endpoint list.       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:showEndpointDetail | Grants permission to query Kubernetes endpoint details.        | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listDeployments    | Grants permission to query the Kubernetes Deployment list.     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listStatefulSets   | Grants permission to query the Kubernetes StatefulSet list.    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listDaemonSets     | Grants permission to query the Kubernetes daemon list.         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listJobs           | Grants permission to query the Kubernetes common job list.     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:listCronJobs       | Grants permission to query the Kubernetes scheduled task list. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |

| Action                                    | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                        |
|-------------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------|
| hss:vulnerability:showVulAffectedStatics  | Grants permission to count the servers affected by vulnerabilities. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:vulnerability:listVulHandleTask       | Grants permission to query the vulnerability handling task list.    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:vulnerability:listVulHandleTaskDetail | Grants permission to query vulnerability handling task details.     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:container:isolateK8sContainer         | Grants permission to modify the status of container.                | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:set</li> </ul>         |
| hss:container:getNetworkStatistics        | Grants permission to query container firewall status.               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |
| hss:container:getClusters                 | Grants permission to query cluster list.                            | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |
| hss:container:getClusterNetworkInfo       | Grants permission to query cluster network information.             | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:read</li> </ul> |

| Action                              | Description                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                        |
|-------------------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------|
| hss:container:getClusterPolicyList  | Grants permission to query container network policy list. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |
| hss:container:deletePolicy          | Grants permission to delete container network policy.     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:delete</li> </ul>  |
| hss:container:createPolicy          | Grants permission to create container network policy.     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:set</li> </ul>  |
| hss:container:updatePolicy          | Grants permission to update container network policy.     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:set</li> </ul>  |
| hss:container:syncClusterPolicyList | Grants permission to sync container network policy.       | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:read</li> </ul> |
| hss:container:syncClusterList       | Grants permission to sync cluster namespace information.  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:read</li> </ul> |
| hss:container:getNamespaceList      | Grants permission to query cluster namespace list.        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |

| Action                                           | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                        |
|--------------------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------|
| hss:container:getNodeList                        | Grants permission to query cluster node list.                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |
| hss:container:syncClusterNodeList                | Grants permission to sync cluster node list.                      | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:read</li> </ul> |
| hss:vulnerability:getVulScanTaskEstimatedTime    | Grants permission to query estimated vulnerability scan duration. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>              |
| hss:antiransomware:addRansomwareProtectionPolicy | Grants permission to add ransomware protection policies.          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>     |
| hss:antiransomware:associateBackupPolicy         | Grants permission to apply backup policies to vaults.             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>     |
| hss:antiransomware:listBackupPolicy              | Grants permission to query the backup policy list.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul>    |
| hss:antiransomware:associateProtectionPolicy     | Grants permission to switch ransomware protection policies.       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>     |
| hss:antiransomware:batchStartProtection          | Grants permission to enable ransomware protection.                | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul>     |

| Action                               | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|--------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:event:getEventAttCk              | Grants permission to query the list of ATT&CK attack phase statistics.                | List         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>     |
|                                      |                                                                                       |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                     |
| hss:event:downloadEventSourceFile    | Grants permission to download alarm source files.                                     | List         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>     |
|                                      |                                                                                       |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                     |
| hss:overview:showSecurityScore       | Grants permission to query security scores.                                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:listSecurityRisk        | Grants permission to query the security risk list.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:showQuotaHostStatistics | Grants permission to query server quota statistics.                                   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:showAgentStatistics     | Grants permission to query the numbers of agents to be upgraded, online, and offline. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:showHotInformation      | Grants permission to query hot news.                                                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |

| Action                             | Description                                                                                                                                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:overview:showSecurityRisk      | Grants permission to query security risk information.                                                                                                                                                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:showProtectStatistics | Grants permission to query the protection period, virus library update time, vulnerability library update time, and accumulated number of records of each module.                                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:overview:showStatistics        | Grants permission to query the numbers of servers with enabled ransomware protection, application protection, web tamper protection, and two-factor authentication; and the number of isolated files. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:overview:list</li> </ul> |
| hss:event:listEventHandleHistory   | Grants permission to query the list of historical events handling.                                                                                                                                    | List         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>     |
|                                    |                                                                                                                                                                                                       |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                     |

| Action                             | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                              |
|------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------|
| hss:image:listSwrlImageRepository  | Grants permission to query the image list in the SWR image repository.                       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:batchScanSwrlImage       | Grants permission to scan images in the image repository in batches.                         | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: set</li> </ul>  |
| hss:image:vulnerabilities          | Grants permission to query image vulnerability details.                                      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listVulnerabilityCVE     | Grants permission to query CVE details about a vulnerability.                                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:listImageRiskConfigRules | Grants permission to query the check items of a specified image security configuration item. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: list</li> </ul> |
| hss:image:runImageSynchronize      | Grants permission to synchronize the image list from SWR.                                    | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images: set</li> </ul>  |

| Action                             | Description                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|------------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:event:listEventForensic        | Grants permission to query event forensics information.    | List         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>           |
|                                    |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                           |
| hss:event:listSimilarHandledEvents | Grants permission to query similar handled alarms.         | List         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>           |
|                                    |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                           |
| hss:event:listSameEvent            | Grants permission to query the same alarms.                | List         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul>           |
|                                    |                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                           |
| hss:container:getPolicies          | Grants permission to query the policy list.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |
| hss:container:getPolicyDetail      | Grants permission to query policy details.                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |
| hss:container:getOverview          | Grants permission to query cluster protection overview.    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |
| hss:container:getProtectEvents     | Grants permission to query cluster protection events.      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |
| hss:container:getProtectClusters   | Grants permission to query cluster protection information. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |



| Action                                           | Description                                                                                             | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:container:changeProtectStatus                | Grants permission to change the cluster protection status.                                              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |
| hss:container:addWhitelma<br>ge                  | Grants permission to add images to the whitelist.                                                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:set</li> </ul>  |
| hss:container:l<br>istDefaultPoli<br>cy          | Grants permission to query the default policy template.                                                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |
| hss:container:l<br>istProtectionI<br>tem         | Grants permission to query the protection scope.                                                        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:clusterProtect:list</li> </ul> |
| hss:vulnerabili<br>ty:getVulBack<br>upStatistics | Grants permission to query backup statistics of the server corresponding to the vulnerability handling. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>           |
| hss:vulnerabili<br>ty:ListVulHost<br>Vaults      | Grants permission to query the list of server vaults corresponding to vulnerability handling.           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>           |

| Action                                 | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                           |
|----------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------|
| hss:vulnerability:ListVulHostBackups   | Grants permission to query the list of backups that can be rolled back.        | List         | host *                      | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul> |
| hss:vulnerability:RestoreVulHostBackup | Grants permission to roll back with backups.                                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>  |
| hss:event:exportEvent                  | Grants permission to export event alarms.                                      | Write        | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul> |
|                                        |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:event:queryExportTask              | Grants permission to query the task of exporting event alarms.                 | Read         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
|                                        |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:event:downloadEvent                | Grants permission to download event alarms.                                    | Read         | event *                     | -                                     | <ul style="list-style-type: none"> <li>hss:event:get</li> </ul> |
|                                        |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:ars:createAppWhitelistPolicy       | Grants permission to create an application process whitelist policy.           | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>   |
|                                        |                                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                 |
| hss:ars:listAppWhitelistPolicy         | Grants permission to query the list of application process whitelist policies. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>  |

| Action                               | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                          |
|--------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------|
| hss:ars:changeAppWhitelistPolicy     | Grants permission to modify an application process whitelist policy.                          | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>  |
|                                      |                                                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                |
| hss:ars:deleteAppWhitelistPolicy     | Grants permission to delete an application process whitelist policy.                          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>  |
| hss:ars:showAppWhitelistPolicy       | Grants permission to query the application process whitelist policy information.              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul> |
| hss:ars:switchAppWhitelistPolicyHost | Grants permission to modify the protection status of an application process whitelist policy. | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>  |
|                                      |                                                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                |
| hss:ars:addAppWhitelistPolicyHost    | Grants permission to add servers to an application process whitelist policy.                  | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>  |
|                                      |                                                                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                |

| Action                                | Description                                                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                          |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------|
| hss:ars:listAppWhitelistPolicyHost    | Grants permission to query the list of servers that an application process whitelist policy applies to.   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul> |
| hss:ars:deleteAppWhitelistPolicyHost  | Grants permission to remove servers from an application process whitelist policy.                         | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>  |
|                                       |                                                                                                           |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                |
| hss:ars:listAppWhitelistHostStatus    | Grants permission to query the list of available servers for an application process whitelist policy.     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul> |
| hss:ars:listAppWhitelistPolicyProcess | Grants permission to query the list of processes that an application process whitelist policy applies to. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul> |

| Action                                        | Description                                                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                          |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------|
| hss:ars:changeAppWhitelistPolicyProcessStatus | Grants permission to modify the process trust status of an application process whitelist policy.           | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>  |
| hss:ars:addAppWhitelistPolicyProcess          | Grants permission to add processes to an application process whitelist policy.                             | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>  |
|                                               |                                                                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                |
| hss:ars:listAppWhitelistPolicyProcessExtended | Grants permission to query the extended process list for an application process whitelist policy.          | List         | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul> |
|                                               |                                                                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                |
| hss:ars:exportAppWhitelistPolicyProcess       | Grants permission to export the list of processes that an application process whitelist policy applies to. | List         | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul> |
|                                               |                                                                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                |

| Action                                               | Description                                                                                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------|
| hss:ars:switchAppWhitelistPolicyLearnStatus          | Grants permission to modify the learning status of an application process whitelist policy.                                                | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>        |
|                                                      |                                                                                                                                            |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                      |
| hss:ars:showAppWhitelistAgentStatics                 | Grants permission to query the number of servers that are protected by the premium edition and do not support application process control. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>       |
| hss:ars:listAppWhitelistEvent                        | Grants permission to query the list of suspicious process events detected by application process control.                                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>       |
| hss:container:deleteSelfBuildK8sClusterDaemonsetInfo | Grants permission to delete the DaemonSet of an on-premises cluster.                                                                       | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:set</li> </ul> |

| Action                                             | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                 |
|----------------------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------|
| hss:container:saveSelfBuildK8sClusterDaemonsetInfo | Grants permission to save the DaemonSet of an on-premises cluster.  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:set</li> </ul>  |
| hss:container:showSelfBuildK8sClusterDaemonsetInfo | Grants permission to query the DaemonSet of an on-premises cluster. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:get</li> </ul>  |
| hss:container:listSelfBuildK8sClusterInfo          | Grants permission to query the on-premises Kubernetes cluster list. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:list</li> </ul> |
| hss:container:createDaemonset                      | Grants permission to create DaemonSet of a CCE cluster.             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:containers:set</li> </ul>  |
| hss:vulnerability:listVulRepairCmds                | Grants permission to query vulnerability fixing commands.           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>       |
| hss:vulnerability:listUrgentVulnerabilities        | Grants permission to query the emergency vulnerability list.        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>       |
| hss:antivirus:createAntivirusTask                  | Grants permission to create virus scan tasks.                       | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:ars:set</li> </ul>         |
|                                                    |                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                       |

| Action                               | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                         | Alias          |
|--------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------|
| hss:antivirus:listAntivirusTask      | Grants permission to query the virus scan task list.                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:ars:list |
| hss:antivirus:switchAntivirusTask    | Grants permission to cancel virus scan tasks.                            | Write        | host *                      | -                                     | • hss:ars:set  |
|                                      |                                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                |
| hss:antivirus:listAntivirusHost      | Grants permission to query the list of servers available for virus scan. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:ars:list |
| hss:antivirus:createAntivirusPolicy  | Grants permission to create custom virus scan policies.                  | Write        | host *                      | -                                     | • hss:ars:set  |
|                                      |                                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                |
| hss:antivirus:listAntivirusPolicy    | Grants permission to query the list of custom virus scan policies.       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:ars:list |
| hss:antivirus:listAntivirusResult    | Grants permission to query the list of virus scan results.               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:ars:list |
| hss:antivirus:operateAntivirusResult | Grants permission to handle virus scan results.                          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:ars:set  |
| hss:antivirus:exportAntivirusResult  | Grants permission to export virus scan results.                          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | • hss:ars:set  |



| Action                                     | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|--------------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:antivirus:showAntivirusStatistic       | Grants permission to query virus scan statistics.                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>      |
| hss:image:showImageFullScanProgress        | Grants permission to query the progress of a full image scan.               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>   |
| hss:host:changeHostIgnoreStatus            | Grants permission to ignore or unignore servers.                            | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:hosts:set</li> </ul>     |
|                                            |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                     |
| hss:host:listIgnoreHosts                   | Grants permission to query ignored servers.                                 | List         | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>    |
|                                            |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                     |
| hss:image:batchExportBaselineTask          | Grants permission to export image baseline check results.                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>    |
| hss:image:showImageSecurityReportStatistic | Grants permission to query the number of image scan results to be exported. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:set</li> </ul>    |
| hss:vulnerability:exportVuls               | Grants permission to create vulnerability export tasks.                     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:set</li> </ul>      |
| hss:exportTask:queryExportTask             | Grants permission to query export tasks.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:keyfiles:list</li> </ul> |

| Action                              | Description                                                                                          | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                  |
|-------------------------------------|------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------|
| hss:file:downloadExportedFile       | Grants permission to download files.                                                                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:keyfiles:list</li> </ul>    |
| hss:image:listGlobalVulnerabilities | Grants permission to query vulnerability details about a tenant image.                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>      |
| hss:image:listVulnerabilityImages   | Grants permission to query details about images in the image repository affected by a vulnerability. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>      |
| hss:setting:getPluginInstallScript  | Grants permission to query server plug-in information.                                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:installAgent:get</li> </ul> |
| hss:setting:getPluginList           | Grants permission to query the plug-in installation guide.                                           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:installAgent:get</li> </ul> |
| hss:setting:getAutoOpenQuotaStatus  | Grants permission to query the status of automatic quota binding.                                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>       |

| Action                                | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                             |
|---------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------------------------------------------|
| hss:setting:changeAutoOpenQuotaStatus | Grants permission to modify the status of automatic quota binding.  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>  |
| hss:image:batchExportSWRVulTask       | Grants permission to export SWR image vulnerability scan results.   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul> |
| hss:image:batchExportLocalVulTask     | Grants permission to export local image vulnerability scan results. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul> |
| hss:vulnerability:exportVulReport     | Grants permission to export vulnerability reports in HTML format.   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |
| hss:vulnerability:getVulReportData    | Grants permission to obtain vulnerability reports in PDF format.    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>   |
| hss:setting:getAgentAutoUpgradeStatus | Grants permission to query the status of automatic agent upgrade.   | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>  |

| Action                                           | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                     |
|--------------------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------|
| hss:setting:changeAgentAutoUpgradeStatus         | Grants permission to modify the status of automatic agent upgrade.                           | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:hosts:list</li> </ul>          |
| hss:quota:showProductdataOfferingInfos           | Grants permission to query product information.                                              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:quotas:get</li> </ul>          |
| hss:image:listLocalImageAppInfo                  | Grants permission to query the local image software list.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>         |
| hss:image:listLocalImageAppVulnerabilities       | Grants permission to query a single software vulnerability list for local image.             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:images:list</li> </ul>         |
| hss:antiransomware:getRansomwareProtectionStatus | Grants permission to query ransomware protection status.                                     | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |
| hss:antiransomware:getAutoDeployAgentList        | Grants permission to query servers for which ransomware protection is automatically enabled. | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>hss:antiransomware:list</li> </ul> |

| Action                                       | Description                                                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| hss:antiransomware:updateAutoDeployAgent     | Grants permission to update servers for which ransomware protection is automatically enabled.                | Write        | -                           | -                                     | <ul style="list-style-type: none"> <li>hss:antiransomware:set</li> </ul> |
| hss:vulnerability:getVulIndividualStatistics | Grants permission to query vulnerability statistics.                                                         | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>          |
| hss:vulnerability:getVulAffectedInfo         | Grants permission to query information about vulnerabilities affected servers or vulnerabilities on servers. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:vuls:list</li> </ul>          |
| hss:event:deleteIsolatedFile                 | Grants permission to delete isolation box files.                                                             | Write        | host *                      | -                                     | <ul style="list-style-type: none"> <li>hss:event:set</li> </ul>          |
|                                              |                                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                                                                          |
| hss:antivirus:listAntivirusHandleHistory     | Grants permission to query historical virus scanning and killing records.                                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:ars:list</li> </ul>           |
| hss:decoyport:showStatistics                 | Grants permission to view port honeypot protection statistics.                                               | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:get</li> </ul>      |

| Action                           | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                |
|----------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------------------------------|
| hss:decoypport:showAutoBind      | Grants permission to view the automatic binding status of the port honeypot.          | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoypport:get</li> </ul> |
| hss:decoypport:switchAutoBind    | Grants permission to modify the automatic binding status of the port honeypot.        | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoypport:set</li> </ul> |
| hss:decoypport:showHostList      | Grants permission to view the protected server list of the port honeypot policy.      | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoypport:get</li> </ul> |
| hss:decoypport:listPolicy        | Grants permission to view the policy list of the port honeypot.                       | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoypport:get</li> </ul> |
| hss:decoypport:listAvailableHost | Grants permission to view the list of servers where the port honeypot can be enabled. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoypport:get</li> </ul> |

| Action                          | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                               |
|---------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------|
| hss:decoyport:switchHostPolicy  | Grants permission to switch the port honeypot protection policy of the server.  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:set</li> </ul> |
| hss:decoyport:deleteHostPolicy  | Grants permission to disable the port honeypot protection policy of the server. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:set</li> </ul> |
| hss:decoyport:createPolicy      | Grants permission to add port honeypot policies.                                | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:set</li> </ul> |
| hss:decoyport:modifyPolicy      | Grants permission to edit port honeypot protection policies.                    | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:set</li> </ul> |
| hss:decoyport:showPolicyDetails | Grants permission to view port honeypot policy details.                         | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:get</li> </ul> |
| hss:decoyport:deletePolicy      | Grants permission to delete port honeypot policies.                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:set</li> </ul> |
| hss:decoyport:switchPolicy      | Grants permission to enable or disable the port honeypot policies.              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:decoyport:set</li> </ul> |

| Action                                     | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                        |
|--------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------|
| hss:exportTask:queryLatestExportTaskByType | Grants permission to query the latest export tasks.                    | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:keyfiles:list</li> </ul>          |
| hss:container:createSecurityGroupPolicy    | Grants permission to create security group policies.                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:set</li> </ul>  |
| hss:container:updateSecurityGroupPolicy    | Grants permission to update security group policies.                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:set</li> </ul>  |
| hss:container:getSecurityGroupPolicyList   | Grants permission to query the security group policy list.             | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |
| hss:container:deleteSecurityGroupPolicy    | Grants permission to delete security group policies.                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:set</li> </ul>  |
| hss:container:syncSecurityGroupPolicy      | Grants permission to synchronize security group policies in a cluster. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:read</li> </ul> |
| hss:container:getWorkloadList              | Grants permission to query the workload list.                          | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |
| hss:container:getSecurityGroupList         | Grants permission to query the security group list.                    | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>hss:container-network:list</li> </ul> |



Each API of HSS usually supports one or more actions. [Table 3-171](#) lists the supported actions and dependencies.

**Table 3-171** Actions and dependencies supported by HSS APIs

| API                                                     | Action                                 | Dependencies                |
|---------------------------------------------------------|----------------------------------------|-----------------------------|
| POST /v5/{project_id}/host-management/groups            | hss:host:addHostsGroup                 | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/pwl/{policy_id}/host               | hss:ars:addPWLPolicyHost               | eps:enterpriseProjects:list |
| POST /v5/{project_id}/rasp/policy                       | hss:rasp:addRaspPolicy                 | eps:enterpriseProjects:list |
| POST /v5/{project_id}/report/security-report            | hss:safetyReport:addSecurityReport     | eps:enterpriseProjects:list |
| POST /v5/{project_id}/wtp/{host_id}/timing-off-config   | hss:wtp:addTimingOffConfigInfo         | eps:enterpriseProjects:list |
| POST /v5/{project_id}/wtp/{host_id}/protect-directories | hss:wtp:addWtpHostProtectDirInfo       | eps:enterpriseProjects:list |
| POST /v5/{project_id}/wtp/{host_id}/privileged-process  | hss:wtp:addWtpPrivilegedProcessInfo    | eps:enterpriseProjects:list |
| POST /v5/{project_id}/setting/virus-kill                | hss:setting:changeAutoKillVirusStatus  | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/event/blocked-ip                   | hss:event:changeBlockedIp              | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/setting/malware/collect            | hss:setting:changeMalwareCollectStatus | eps:enterpriseProjects:list |

| API                                                        | Action                                              | Dependencies                |
|------------------------------------------------------------|-----------------------------------------------------|-----------------------------|
| POST /v5/{project_id}/pwl/policy                           | hss:ars:changePWLPolicy                             | eps:enterpriseProjects:list |
| POST /v5/{project_id}/pwl/{policy_id}/process              | hss:ars:changePWLPolicy-ProcessStatus               | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/report/security-report                | hss:safetyReport:changeSecurityReport               | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/pwl/policy                            | hss:ars:createPWLPolicy                             | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/pwl/policy                         | hss:ars:deletePWLPolicy                             | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/pwl/{policy_id}/host               | hss:ars:deletePWLPolicy-Host                        | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/ransomware/duplication/{backup_id} | hss:antiransomware:deleteRansomwareDuplicationInfo  | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/ransomware/protection/policy       | hss:antiransomware:deleteRansomwareProtectionPolicy | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/rasp/policy                        | hss:rasp:deleteRaspPolicy                           | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/report/security-report             | hss:safetyReport:deleteSecurityReport               | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/wtp/{host_id}/timing-off-config    | hss:wtp:deleteTimingOff-ConfigInfo                  | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/wtp/{host_id}/protect-directories  | hss:wtp:deleteWtpHostProtectDirInfo                 | eps:enterpriseProjects:list |

| API                                                      | Action                                         | Dependencies                |
|----------------------------------------------------------|------------------------------------------------|-----------------------------|
| DELETE /v5/{project_id}/wtp/{host_id}/privileged-process | hss:wtp:deleteWtpPrivilegedProcessInfo         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/agent-install-script        | hss:setting:getAgentInstallScript              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/alarm-config                | hss:setting:getAlarmConfig                     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/rasp/{host_id}/status               | hss:rasp:getAppRaspSwitchStatus                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/virus-kill                  | hss:setting:getAutoKillVirusStatus             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/container/node-statistics           | hss:container:getContainerNodeStatistics       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/files/statistic                     | hss:keyfile:getFileStatistic                   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/malware/collect             | hss:setting:getMalwareCollectStatus            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/malware/reminders           | hss:setting:getMalwareReminders                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/security-check/manual-check/status  | hss:securitycheck:getManualSecurityCheckStatus | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/asset/groups/statistics    | hss:overview:getOverviewAssetGroupsStatistics  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/asset/os/statistics        | hss:overview:getOverviewAssetOsStatistics      | eps:enterpriseProjects:list |

| API                                                       | Action                                                | Dependencies                |
|-----------------------------------------------------------|-------------------------------------------------------|-----------------------------|
| GET /v5/{project_id}/overview/asset/statistics            | hss:overview:getOverviewAssetStatistics               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/risk/attck-mitre            | hss:overview:getOverviewAttckMitre                    | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/risk/defense/statistics     | hss:overview:getOverviewDefenseStatistics             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/risk/protection/statistics  | hss:overview:getOverviewProtectionStatusStatistics    | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/quota/statistics            | hss:overview:getOverviewQuotaStatistics               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/risk/lists                  | hss:overview:getOverviewRiskLists                     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/risk/manage/statistics      | hss:overview:getOverviewRiskManageStatistics          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/risk/score                  | hss:overview:getOverviewRiskScore                     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/risk/event/statistics       | hss:overview:getOverviewRiskStatistics                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/overview/trial/statistic             | hss:overview:getOverviewTrialsStatistics              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/backup/{backup_id}/detail | hss:antiransomware:getRansomwareBackupInfoBy-BackupId | eps:enterpriseProjects:list |

| API                                                       | Action                                               | Dependencies                |
|-----------------------------------------------------------|------------------------------------------------------|-----------------------------|
| GET /v5/{project_id}/backup/policy                        | hss:antiransomware:getRansomwareHSSBackupPolicyInfo  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/statistics/backup         | hss:antiransomware:getRansomwareBackupStatistics     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/statistics/protection     | hss:antiransomware:getRansomwareProtectionStatistics | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/backup/vault              | hss:antiransomware:getRansomwareVaultInfo            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/rasp/policy/detail                   | hss:rasp:getRaspPolicyDetail                         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/rasp/statistics                      | hss:rasp:getRaspProtectStatistics                    | eps:enterpriseProjects:list |
| GET /v5/{project_id}/wtp/{host_id}/rasp/status            | hss:wtp:getRaspSwitchStatus                          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/security-check/config                | hss:securitycheck:getSecurityCheckConfig             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/security-check/host-report/{host_id} | hss:securitycheck:getSecurityCheckHostReport         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/security-check/overview              | hss:securitycheck:getSecurityCheckOverview           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/security-check/statistic             | hss:securitycheck:getSecurityCheckStatistic          | eps:enterpriseProjects:list |

| API                                                                     | Action                                         | Dependencies                |
|-------------------------------------------------------------------------|------------------------------------------------|-----------------------------|
| GET /v5/{project_id}/report/security-report                             | hss:safetyReport:getSecurityReport             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/report/report-subscription                         | hss:safetyReport:getSecurityReportSubscription | eps:enterpriseProjects:list |
| GET /v5/{project_id}/wtp/{host_id}/timing-off/status                    | hss:wtp:getTimingOffStatusInfo                 | eps:enterpriseProjects:list |
| GET /v5/{project_id}/wtp/statistics                                     | hss:wtp:getWtpDashboardProtectStatistics       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/wtp/{host_id}/rasp_path                            | hss:wtp:getWtpDirectory                        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/wtp/{host_id}/monitor-only/status                  | hss:wtp:getWtpDirectoryMonitorOnlyStatus       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/webtamper/static/{host_id}/privileged-child/status | hss:wtp:getWtpPrivilegedProcessesChildStatus   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/wtp/{host_id}/backup-host                          | hss:wtp:getWtpRemoteBackupHostInfo             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/agent-version                              | hss:setting:listAgentVersion                   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/container/nodes                                    | hss:container:listContainerNodes               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/files/change-files                                 | hss:keyfile:listFileEvents                     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/{host_id}/files/change-files                       | hss:keyfile:listFileHostEventDetails           | eps:enterpriseProjects:list |

| API                                                | Action                                            | Dependencies                |
|----------------------------------------------------|---------------------------------------------------|-----------------------------|
| GET /v5/{project_id}/files/change-host             | hss:keyfile:listFileHosts                         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/host-management/groups        | hss:host:listHostGroups                           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/login-common-ip       | hss:setting:listLoginCommonIp                     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/login-common-location | hss:setting:listLoginCommonLocation               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/setting/login-white-ip        | hss:setting:listLoginWhiteIp                      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/policy/groups                 | hss:policy:listPolicyGroup                        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/ports/detail            | hss:asset:listPortHost                            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/processes/detail        | hss:asset:listProcessesHost                       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/pwl/event                     | hss:ars:listPWLEvent                              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/pwl/policy                    | hss:ars:listPwlPolicy                             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/pwl/{policy_id}/host          | hss:ars:listPwlPolicyHost                         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/pwl/{policy_id}/process       | hss:ars:listPwlPolicyProcess                      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/backup/{host_id}   | hss:antiransomware:listRansomwareBackedupByHostId | eps:enterpriseProjects:list |

| API                                                               | Action                                                    | Dependencies                |
|-------------------------------------------------------------------|-----------------------------------------------------------|-----------------------------|
| GET /v5/{project_id}/ransomware/backup/operation-logs             | hss:antiransomware:listRansomwareOperationLogsByVaultName | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/optional/server                   | hss:antiransomware:listRansomwareProtectionOptionalServer | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/protection/policy                 | hss:antiransomware:listRansomwareProtectionPolicy         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/server                            | hss:antiransomware:listRansomwareProtectionServer         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/rasp/rule                                    | hss:rasp:listRaspCheckFeatureRule                         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/rasp/events                                  | hss:rasp:listRaspEvents                                   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/rasp/policies                                | hss:rasp:listRaspPolicies                                 | eps:enterpriseProjects:list |
| GET /v5/{project_id}/rasp/servers                                 | hss:rasp:listRaspProtectionServers                        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/security-check/host-report/history/{host_id} | hss:securitycheck:listSecurityCheckHostReportHistory      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/security-check/host-results                  | hss:securitycheck:listSecurityCheckHostResult             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/report/report-list                           | hss:safetyReport:listSecurityReport                       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/report/period-list                           | hss:safetyReport:listSecurityReportHistoryPeriod          | eps:enterpriseProjects:list |



| API                                                    | Action                                           | Dependencies                                                                                          |
|--------------------------------------------------------|--------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| GET /v5/{project_id}/report/sending-list               | hss:safetyReport:listSecurityReportSendingRecord | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/wtp/{host_id}/timing-off-config   | hss:wtp:listTimingOffConfigInfo                  | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/setting/two-factor-login/hosts    | hss:setting:listTwoFactorLoginHost               | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/wtp/backup-hosts                  | hss:wtp:listWtpBackupHostsInfo                   | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/wtp/{host_id}/protect-directories | hss:wtp:listWtpHostProtectDirInfo                | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/webtamper/static/protect-history  | hss:wtp:listWtpHostProtectHistoryInfo            | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/webtamper/rasp/protect-history    | hss:wtp:listWtpHostRaspProtectHistoryInfo        | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/wtp/{host_id}/privileged-process  | hss:wtp:listWtpPrivilegedProcessesInfo           | eps:enterpriseProjects:list                                                                           |
| GET /v5/{project_id}/webtamper/hosts                   | hss:wtp:listWtpProtectHost                       | <ul style="list-style-type: none"> <li>eps:enterpriseProjects:list</li> <li>vpc:ports:list</li> </ul> |
| POST /v5/{project_id}/setting/login-common-ip          | hss:setting:modifyLoginCommonIp                  | eps:enterpriseProjects:list                                                                           |
| POST /v5/{project_id}/setting/login-common-location    | hss:setting:modifyLoginCommonLocation            | eps:enterpriseProjects:list                                                                           |
| POST /v5/{project_id}/setting/login-white-ip           | hss:setting:modifyLoginWhitelip                  | eps:enterpriseProjects:list                                                                           |

| API                                                              | Action                                              | Dependencies                |
|------------------------------------------------------------------|-----------------------------------------------------|-----------------------------|
| POST /v5/{project_id}/pwl/event/operate                          | hss:ars:operatePWLEvent                             | eps:enterpriseProjects:list |
| POST /v5/{project_id}/pwl/{policy_id}/relearn                    | hss:ars:relearnPWLPolicy                            | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/overview/risk/score                         | hss:overview:resetOverviewRiskScore                 | eps:enterpriseProjects:list |
| POST /v5/{project_id}/ransomware/duplication/{backup_id}/restore | hss:antiransomware:restoreRansomwareDuplicationInfo | eps:enterpriseProjects:list |
| POST /v5/{project_id}/report/sending                             | hss:safetyReport:sendSecurityReport                 | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/setting/reminders-config                    | hss:setting:setAlarmConfig                          | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/setting/malware/reminders                   | hss:setting:setMalwareReminders                     | eps:enterpriseProjects:list |
| POST /v5/{project_id}/wtp/{host_id}/set-remote-backup            | hss:wtp:setRemoteWtpBackupInfo                      | eps:enterpriseProjects:list |
| POST /v5/{project_id}/wtp/{host_id}/timing-off/status            | hss:wtp:setTimingOffSwitchInfo                      | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/setting/two-factor-login/config             | hss:setting:setTwoFactorLoginConfig                 | eps:enterpriseProjects:list |
| POST /v5/{project_id}/wtp/{host_id}/monitor-only/status          | hss:wtp:setWtpDirectory-MonitorOnlyStatus           | eps:enterpriseProjects:list |

| API                                                                      | Action                                                       | Dependencies                |
|--------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------|
| POST /v5/{project_id}/webtamper/static/{host_id}/privileged-child/status | hss:wtp:setWtpPrivileged-ProcessesChildStatus                | eps:enterpriseProjects:list |
| POST /v5/{project_id}/webtamper/static/status                            | hss:wtp:setWtpProtection-StatusInfo                          | eps:enterpriseProjects:list |
| POST /v5/{project_id}/webtamper/rasp/status                              | hss:wtp:setWtpProtectSwitc<br>h                              | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/wtp/{host_id}/date-off-config                       | hss:wtp:setWtpScheduled-<br>ProtectionDateOffConfigIn-<br>fo | eps:enterpriseProjects:list |
| POST /v5/{project_id}/security-check/manual-check/start                  | hss:securitycheck:startManu<br>alSecurityCheck               | eps:enterpriseProjects:list |
| POST /v5/{project_id}/ransomware/backup/open/{host_id}                   | hss:antiransomware:startRa<br>nsomwareBackupSingle           | eps:enterpriseProjects:list |
| POST /v5/{project_id}/ransomware/protection/open                         | hss:antiransomware:startRa<br>nsomwareProtection             | eps:enterpriseProjects:list |
| POST /v5/{project_id}/ransomware/protection/open/{host_id}               | hss:antiransomware:startRa<br>nsomwareProtectionSingle       | eps:enterpriseProjects:list |
| POST /v5/{project_id}/security-check/manual-check/stop                   | hss:securitycheck:stopManu<br>alSecurityCheck                | eps:enterpriseProjects:list |
| POST /v5/{project_id}/ransomware/protection/close                        | hss:antiransomware:stopRa<br>nsomwareProtection              | eps:enterpriseProjects:list |

| API                                                            | Action                                              | Dependencies                |
|----------------------------------------------------------------|-----------------------------------------------------|-----------------------------|
| POST /v5/{project_id}/container/switch-version                 | hss:container:switchContainerProtectStatus          | eps:enterpriseProjects:list |
| POST /v5/{project_id}/pwl/{policy_id}/host                     | hss:ars:switchPWLPolicy-Host                        | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/rasp/status                               | hss:rasp:switchRasp                                 | eps:enterpriseProjects:list |
| POST /v5/{project_id}/report/report-status                     | hss:safetyReport:switchSecurityReportStatus         | eps:enterpriseProjects:list |
| POST /v5/{project_id}/wtp/{host_id}/protect-directories/status | hss:wtp:switchWtpHostProtectDirInfo                 | eps:enterpriseProjects:list |
| POST /v5/{project_id}/host-management/uninstall                | hss:host:uninstallAgents                            | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/setting/alarm-config                      | hss:setting:updateAlarmConfig                       | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/backup/policy                             | hss:antiransomware:updateRansomwareBackupPolicyInfo | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/ransomware/protection/policy              | hss:antiransomware:updateRansomwareProtectionPolicy | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/rasp/policy                               | hss:rasp:updateRaspPolicy                           | eps:enterpriseProjects:list |
| POST /v5/{project_id}/security-check/config                    | hss:securitycheck:updateSecurityCheckConfig         | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/wtp/{host_id}/timing-off-config           | hss:wtp:updateTimingOff-ConfigInfo                  | eps:enterpriseProjects:list |

| API                                                          | Action                                 | Dependencies                |
|--------------------------------------------------------------|----------------------------------------|-----------------------------|
| PUT /v5/{project_id}/wtp/backup-hosts                        | hss:wtp:updateWtpBackupHostInfo        | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/wtp/{host_id}/rasp_path                 | hss:wtp:updateWtpDirectoryInfo         | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/wtp/{host_id}/protect-directories       | hss:wtp:updateWtpHostProtectDirInfo    | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/wtp/{host_id}/privileged-process        | hss:wtp:updateWtpPrivilegedProcessInfo | eps:enterpriseProjects:list |
| POST /v5/{project_id}/asset/values/host                      | hss:asset:addValuesLevel               | eps:enterpriseProjects:list |
| POST /v5/{project_id}/asset/batch-modify-port-status         | hss:asset:batchModifyPortStatus        | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/investigation/tool/condition-history | hss:asset:deleteToolConditionHistory   | eps:enterpriseProjects:list |
| POST /v5/{project_id}/investigation/tool/execute             | hss:asset:executeTool                  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/account   | hss:asset:getAccountTop                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/status/agent             | hss:asset:getAgentStatisticsStatus     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/statistics                        | hss:asset:getAssetStatistic            | eps:enterpriseProjects:list |

| API                                                               | Action                                        | Dependencies                |
|-------------------------------------------------------------------|-----------------------------------------------|-----------------------------|
| GET /v5/{project_id}/asset/overview/status/type                   | hss:asset:getAssetType                        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/auto-launch    | hss:asset:getAutoLaunchTo<br>p                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/common-port-info                       | hss:asset:getCommonPort                       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/status/container/protection   | hss:asset:getContainerPro-<br>tectionStatus   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/core-conf-file | hss:asset:getCoreConfFile-<br>Top             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/environment    | hss:asset:getEnvironmentTo<br>p               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/manual-collect/{type}                  | hss:asset:getHostAssetMan<br>ualCollectStatus | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/status/host/protection        | hss:asset:getHostProtection<br>Status         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/jar-package    | hss:asset:getJarPackageTop                    | eps:enterpriseProjects:list |

| API                                                                    | Action                           | Dependencies                |
|------------------------------------------------------------------------|----------------------------------|-----------------------------|
| GET /v5/{project_id}/asset/overview/statistics/top/kernel-module       | hss:asset:getKernelModule-Top    | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/status/os                          | hss:asset:getOsStatisticsInfo    | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/process             | hss:asset:getPorcessTop          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/port                | hss:asset:getPortTop             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/status/quota                       | hss:asset:getQuotaStatistic-Info | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/software            | hss:asset:getSoftwareTop         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/web-app-and-service | hss:asset:getWebAppAndServiceTop | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/web-app             | hss:asset:getWebAppTop           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/web-framework       | hss:asset:getWebFrameworkTop     | eps:enterpriseProjects:list |

| API                                                            | Action                                  | Dependencies                |
|----------------------------------------------------------------|-----------------------------------------|-----------------------------|
| GET /v5/{project_id}/asset/overview/statistics/top/web-service | hss:asset:getWebServiceTop              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/overview/statistics/top/web-site    | hss:asset:getWebSiteTop                 | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/app/change-history                  | hss:asset:listAppChangeHistories        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/apps                                | hss:asset:listApps                      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/app/statistics                      | hss:asset:listAppStatistics             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/auto-launch/change-history          | hss:asset:listAutoLaunchChangeHistories | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/auto-launches                       | hss:asset:listAutoLaunchs               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/auto-launch/statistics              | hss:asset:listAutoLaunchStatistics      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/host/core-conf-file                 | hss:asset:listCoreConfFileHostInfo      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/core-conf-file            | hss:asset:listCoreConfFileInfo          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/statistics/core-conf-file           | hss:asset:listCoreConfFileStatistics    | eps:enterpriseProjects:list |



| API                                                 | Action                               | Dependencies                |
|-----------------------------------------------------|--------------------------------------|-----------------------------|
| GET /v5/{project_id}/asset/host/environment         | hss:asset:listEnvironmentHostInfo    | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/environment    | hss:asset:listEnvironmentInfo        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/statistics/environment   | hss:asset:listEnvironmentStatistics  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/midwares/detail          | hss:asset:listJarPackageHostInfo     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/jar-package    | hss:asset:listJarPackageInfo         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/midwares                 | hss:asset:listJarPackageStatistics   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/host/kernel-module       | hss:asset:listKernelModuleHostInfo   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/kernel-module  | hss:asset:listKernelModuleInfo       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/statistics/kernel-module | hss:asset:listKernelModuleStatistics | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/ports                    | hss:asset:listPorts                  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/port/statistics          | hss:asset:listPortStatistics         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/processes                | hss:asset:listProcesses              | eps:enterpriseProjects:list |

| API                                                       | Action                                   | Dependencies                |
|-----------------------------------------------------------|------------------------------------------|-----------------------------|
| GET /v5/{project_id}/asset/process/statistics             | hss:asset:listProcessStatistics          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/investigation/tool/result            | hss:asset:listResult                     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/investigation/tool/list              | hss:asset:listTool                       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/investigation/tool/condition-history | hss:asset:listToolConditionHistory       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/user/change-history            | hss:asset:listUserChangeHistories        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/userGroup                      | hss:asset:listUserGroup                  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/users                          | hss:asset:listUsers                      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/user/statistics                | hss:asset:listUserStatistics             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/web-app-and-services           | hss:asset:listWebAppAndServices          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/web-app-and-service-statistics | hss:asset:listWebAppAndServiceStatistics | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/host/web-app                   | hss:asset:listWebAppHostInfo             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/web-app              | hss:asset:listWebAppInfo                 | eps:enterpriseProjects:list |

| API                                                 | Action                               | Dependencies                |
|-----------------------------------------------------|--------------------------------------|-----------------------------|
| GET /v5/{project_id}/asset/statistics/web-app       | hss:asset:listWebAppStatistics       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/host/web-framework       | hss:asset:listWebFrameworkHostInfo   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/web-framework  | hss:asset:listWebFrameworkInfo       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/statistics/web-framework | hss:asset:listWebFrameworkStatistics | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/host/web-service         | hss:asset:listWebServiceHostInfo     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/web-service    | hss:asset:listWebServiceInfo         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/statistics/web-service   | hss:asset:listWebServiceStatistics   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/host/web-site            | hss:asset:listWebSiteHostInfo        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/{host_id}/web-site       | hss:asset:listWebSiteInfo            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/asset/statistics/web-site      | hss:asset:listWebSiteStatistics      | eps:enterpriseProjects:list |
| POST /v5/{project_id}/asset/manual-collect/{type}   | hss:asset:runHostAssetManualCollect  | eps:enterpriseProjects:list |

| API                                                                      | Action                                      | Dependencies                |
|--------------------------------------------------------------------------|---------------------------------------------|-----------------------------|
| POST /v5/{project_id}/baseline/security-checks/policy-group/add          | hss:baseline:addSecurityCheckPolicyGroup    | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/baseline/check-rule/action                          | hss:baseline:changeCheckRuleState           | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/baseline/security-checks/policy-group/{group_id} | hss:baseline:deleteSecurityCheckPolicyGroup | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/risk-config/export                         | hss:baseline:exportSecurityCheckReport      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/overview                                   | hss:baseline:getBaselineOverview            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/scan-status                                | hss:baseline:getBaselineScanStatus          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/statistic                                  | hss:baseline:getBaselineStatistic           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/check-rule/detail                          | hss:baseline:getCheckRuleDetail             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/check-rule/fail-detail                     | hss:baseline:getCheckRuleFailDetail         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/security-checks/default-policy             | hss:baseline:getDefaultSecurityCheckPolicy  | eps:enterpriseProjects:list |

| API                                                                  | Action                                            | Dependencies                |
|----------------------------------------------------------------------|---------------------------------------------------|-----------------------------|
| GET /v5/{project_id}/baseline/security-checks/default-policy/details | hss:baseline:getDefaultSecurityCheckPolicyDetails | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/risk-config/{check_name}/detail        | hss:baseline:getRiskConfigDetail                  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/check-rule/hosts                       | hss:baseline:listCheckRuleHosts                   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/password-complexity                    | hss:baseline:listPasswordComplexity               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/risk-config/{check_name}/check-rules   | hss:baseline:listRiskConfigCheckRules             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/risk-config/{check_name}/hosts         | hss:baseline:listRiskConfigHosts                  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/risk-configs                           | hss:baseline:listRiskConfigs                      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/security-checks/policy-groups          | hss:baseline:listSecurityCheckPolicyGroup         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/weak-password-users                    | hss:baseline:listWeakPasswordUsers                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/baseline/detection/{group_id}                   | hss:baseline:runBaselineDetect                    | eps:enterpriseProjects:list |

| API                                                                    | Action                                      | Dependencies                |
|------------------------------------------------------------------------|---------------------------------------------|-----------------------------|
| POST /v5/{project_id}/baseline/security-checks/policy-group/{group_id} | hss:baseline:updateSecurityCheckPolicyGroup | eps:enterpriseProjects:list |
| POST /v5/{project_id}/event/white-list/login                           | hss:event:addLoginWhiteList                 | eps:enterpriseProjects:list |
| POST /v5/{project_id}/event/batch-operate                              | hss:event:batchChangeEvent                  | eps:enterpriseProjects:list |
| POST /v5/{project_id}/event/operate                                    | hss:event:changeEvent                       | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/event/isolated-file                               | hss:event:changeIsolatedFile                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/white-list/export                           | hss:event:exportAlarmWhiteList              | eps:enterpriseProjects:list |
| POST /v5/{project_id}/emergency/event/export                           | hss:event:exportEmergency                   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/emergency/event/emergency-statistics              | hss:event:getEmergencyStatistics            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/attack-tag                                  | hss:event:getEventAttackTag                 | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/severity                                    | hss:event:getEventSeverity                  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/statistics                                  | hss:event:getEventStatistics                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/emergency/event/event-detail                      | hss:event:getMalwareInfo                    | eps:enterpriseProjects:list |

| API                                                        | Action                            | Dependencies                |
|------------------------------------------------------------|-----------------------------------|-----------------------------|
| POST /v5/{project_id}/emergency/event/handle-malware-event | hss:event:handleMalwareEvent      | eps:enterpriseProjects:list |
| POST /v5/{project_id}/event/white-list/import              | hss:event:importAlarmWhiteList    | eps:enterpriseProjects:list |
| POST /v5/{project_id}/emergency/event/isolate-operate      | hss:event:isolateOperateEmergency | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/white-list/alarm                | hss:event:listAlarmWhiteList      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/blocked-ip                      | hss:event:listBlockedIp           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/batch-operate                   | hss:event:listEventOperates       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/top-risk                        | hss:event:listEventTopRisk        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/event-type                      | hss:event:listEventType           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/emergency/event/file-isolate-list     | hss:event:listFileIsolateList     | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/isolated-file                   | hss:event:listIsolatedFile        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/white-list/login                | hss:event:listLoginWhiteList      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/emergency/event/event-list            | hss:event:listMalware             | eps:enterpriseProjects:list |

| API                                                        | Action                           | Dependencies                                                                                                                   |
|------------------------------------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| GET /v5/{project_id}/event/events                          | hss:event:listSecurityEvents     | eps:enterpriseProjects:list                                                                                                    |
| POST /v5/{project_id}/emergency/event/recover-isolate-file | hss:event:recoverIsolateFile     | eps:enterpriseProjects:list                                                                                                    |
| DELETE /v5/{project_id}/event/white-list/alarm             | hss:event:removeAlarmWhiteList   | eps:enterpriseProjects:list                                                                                                    |
| DELETE /v5/{project_id}/event/white-list/login             | hss:event:removeLoginWhiteList   | eps:enterpriseProjects:list                                                                                                    |
| PUT /v5/{project_id}/host-management/asset-value/associate | hss:host:associateHostAssetValue | eps:enterpriseProjects:list                                                                                                    |
| POST /v5/{project_id}/host-management/group/associate      | hss:host:associateHostsGroup     | eps:enterpriseProjects:list                                                                                                    |
| POST /v5/{project_id}/setting/batch-install-agent          | hss:host:batchInstallAgent       | <ul style="list-style-type: none"> <li>• eps:enterpriseProjects:list</li> <li>• ecs:cloudServers:listServersDetails</li> </ul> |
| PUT /v5/{project_id}/host-management/groups                | hss:host:changeHostsGroup        | eps:enterpriseProjects:list                                                                                                    |
| DELETE /v5/{project_id}/host-management/groups             | hss:host:deleteHostsGroup        | eps:enterpriseProjects:list                                                                                                    |
| GET /v5/{project_id}/host-management/host-statistics       | hss:host:getHostsStatistics      | eps:enterpriseProjects:list                                                                                                    |
| GET /v5/{project_id}/host-management/firewall              | hss:host:listFirewallStatus      | eps:enterpriseProjects:list                                                                                                    |



| API                                                    | Action                            | Dependencies                                                                                                                      |
|--------------------------------------------------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| GET /v5/{project_id}/host-management/asset-value       | hss:host:listHostGroupAssetValue  | eps:enterpriseProjects:list                                                                                                       |
| GET /v5/{project_id}/host-management/hosts-risk        | hss:host:listHostsRisk            | <ul style="list-style-type: none"> <li>eps:enterpriseProjects:list</li> <li>vpc:ports:list</li> <li>eip:publicIps:list</li> </ul> |
| GET /v5/{project_id}/host-management/hosts             | hss:host:listHostStatus           | <ul style="list-style-type: none"> <li>eps:enterpriseProjects:list</li> <li>vpc:ports:list</li> <li>eip:publicIps:list</li> </ul> |
| GET /v5/{project_id}/upgrade/agent-upgrade             | hss:host:listHostsUpgrade         | eps:enterpriseProjects:list                                                                                                       |
| POST /v5/{project_id}/vulnerability/scan-task          | hss:host:manualCheckVul           | eps:enterpriseProjects:list                                                                                                       |
| POST /v5/{project_id}/host-management/firewall         | hss:host:switchFirewallStatus     | eps:enterpriseProjects:list                                                                                                       |
| POST /v5/{project_id}/host-management/protection       | hss:host:switchHostsProtectStatus | eps:enterpriseProjects:list                                                                                                       |
| POST /v5/{project_id}/upgrade/agent-upgrade            | hss:host:upgradeAgent             | eps:enterpriseProjects:list                                                                                                       |
| POST /v5/{project_id}/host-management/upgrade          | hss:host:upgradeAgents            | eps:enterpriseProjects:list                                                                                                       |
| POST /v5/{project_id}/image/local/batch-scan           | hss:image:batchScanLocalImage     | eps:enterpriseProjects:list                                                                                                       |
| GET /v5/{project_id}/image/{image_id}/files-statistics | hss:image:getImageFilesStat       | eps:enterpriseProjects:list                                                                                                       |

| API                                            | Action                              | Dependencies                |
|------------------------------------------------|-------------------------------------|-----------------------------|
| GET /v5/{project_id}/image/local/vul/overview  | hss:image:getImageLocalVulOverview  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/vul/overview        | hss:image:getImageVulOverview       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/baseline/affected   | hss:image:listCfgCheckAffectedImage | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/baseline            | hss:image:listGlobalCfgCheck        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/malwares            | hss:image:listGlobalMalware         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/vuls                | hss:image:listGlobalVul             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/{image_id}/apps     | hss:image:listImageApps             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/{image_id}/app/vuls | hss:image:listImageAppVul           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/{image_id}/baseline | hss:image:listImageCfgCheck         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/{image_id}/files    | hss:image:listImageFiles            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/local-repository    | hss:image:listImageLocal            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/{image_id}/malwares | hss:image:listImageMalware          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/namespace           | hss:image:listImageNamespace        | eps:enterpriseProjects:list |

| API                                                    | Action                               | Dependencies                |
|--------------------------------------------------------|--------------------------------------|-----------------------------|
| GET /v5/{project_id}/image/repos                       | hss:image:listImageRepository        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/instance/{instance_id}/image/vuls | hss:image:listInstanceImageVul       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/local/containers            | hss:image:listLocalImageContainers   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/local/hosts                 | hss:image:listLocalImageHosts        | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/local/malware               | hss:image:listLocalImageMalware      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/local/vuls                  | hss:image:listLocalImageVuls         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/local/{vul_id}/images       | hss:image:listLocalVulRepoImage      | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/shared-repository           | hss:image:listSharedImageRepository  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/{vul_id}/images             | hss:image:listVulRepoImage           | eps:enterpriseProjects:list |
| POST /v5/{project_id}/image/vul-task                   | hss:image:runImageScan               | eps:enterpriseProjects:list |
| POST /v5/{project_id}/image/swr/vul-task               | hss:image:runSwrImageScan            | eps:enterpriseProjects:list |
| POST /v5/{project_id}/image/shared-synchronize-task    | hss:image:sharedImageSynchronization | eps:enterpriseProjects:list |

| API                                                               | Action                             | Dependencies                |
|-------------------------------------------------------------------|------------------------------------|-----------------------------|
| PUT /v5/{project_id}/policy/group                                 | hss:policy:addPolicyGroup          | eps:enterpriseProjects:list |
| POST /v5/{project_id}/policy/deploy                               | hss:policy:associatePolicyGroup    | eps:enterpriseProjects:list |
| POST /v5/{project_id}/policy/{policy_id}                          | hss:policy:changePolicyDetail      | eps:enterpriseProjects:list |
| POST /v5/{project_id}/policy/group                                | hss:policy:changePolicyGroup       | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/policy/group                              | hss:policy:deletePolicyGroup       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/policy/{policy_id}                           | hss:policy:getPolicyDetail         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/policy/group/{group_id}                      | hss:policy:listPolicyGroupDetail   | eps:enterpriseProjects:list |
| POST /v5/{project_id}/{resource_type}/{resource_id}/tags          | hss:quota:addResourceInstanceTag   | eps:enterpriseProjects:list |
| POST /v5/{project_id}/{resource_type}/{resource_id}/tags/create   | hss:quota:batchCreateTags          | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/{resource_type}/{resource_id}/tags/delete | hss:quota:batchDeleteTags          | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/billing/quotas                               | hss:quota:cancelHostsQuota         | eps:enterpriseProjects:list |
| POST /v1/{project_id}/hss/{resource_id}/tags/action               | hss:quota:changeTmsResourceTagInfo | eps:enterpriseProjects:list |

| API                                                              | Action                                 | Dependencies                |
|------------------------------------------------------------------|----------------------------------------|-----------------------------|
| POST /v5/{project_id}/{resource_type}/resource-instances/count   | hss:quota:countResourceInstances       | eps:enterpriseProjects:list |
| DELETE /v5/{project_id}/{resource_type}/{resource_id}/tags/{key} | hss:quota:deleteResourceInstanceTag    | eps:enterpriseProjects:list |
| POST /v5/{project_id}/{resource_type}/resource-instances/filter  | hss:quota:filterResourceInstanceList   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/{resource_type}/{resource_id}/tags          | hss:quota:getResourceInstanceTag       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/billing/quotas                              | hss:quota:getResourceQuotas            | eps:enterpriseProjects:list |
| GET /v1/{project_id}/hss/{resource_id}/tags                      | hss:quota:getTmsResourceTagsInfo       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/{resource_type}/tags                        | hss:quota:listProjectTags              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/billing/quotas-detail                       | hss:quota:listQuotasDetail             | eps:enterpriseProjects:list |
| POST /v5/{project_id}/billing/resource-id-list                   | hss:quota:listResourceIds              | eps:enterpriseProjects:list |
| POST /v1/{project_id}/hss/resource-instances/action              | hss:quota:listTmsResourceInstancesInfo | eps:enterpriseProjects:list |
| POST /v5/{project_id}/hss/upgrade_orders/{order_id}              | hss:quota:upgradeOrder                 | eps:enterpriseProjects:list |

| API                                               | Action                                           | Dependencies                |
|---------------------------------------------------|--------------------------------------------------|-----------------------------|
| PUT /v5/{project_id}/vulnerability/status         | hss:vulnerability:changeVulStatus                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/emergency/list           | hss:vulnerability:exportEmergencyVulnerabilities | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/export-vuls-list         | hss:vulnerability:exportVulsList                 | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/cms-detail               | hss:vulnerability:getCmsVulDetail                | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/emergency/summary        | hss:vulnerability:getEmergencySummary            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/emergency/detail         | hss:vulnerability:getEmergencyVulDetail          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/linux-detail             | hss:vulnerability:getLinuxVulDetail              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/manual/scan/status       | hss:vulnerability:getVulCheckStatus              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/vul-summary              | hss:vulnerability:getVulSummary                  | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/windows-detail           | hss:vulnerability:getWindowsVulDetail            | eps:enterpriseProjects:list |
| GET /v5/{project_id}/windows/vul/num              | hss:vulnerability:getWindowsVulNum               | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vulnerability/host/{host_id} | hss:vulnerability:listHostVuls                   | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/host-summary             | hss:vulnerability:listHostVulSummary             | eps:enterpriseProjects:list |

| API                                                           | Action                                      | Dependencies                |
|---------------------------------------------------------------|---------------------------------------------|-----------------------------|
| GET /v5/{project_id}/vul/top-vul                              | hss:vulnerability:listTopVulSummary         | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vulnerability/hosts                      | hss:vulnerability:listVulHosts              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vulnerability/vulnerabilities            | hss:vulnerability:listVulnerabilities       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/{host_id}/fail_detail                | hss:vulnerability:listVulRepairFailedDetail | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vul/vul-type-summary                     | hss:vulnerability:listVulTypeSummary        | eps:enterpriseProjects:list |
| POST /v5/{project_id}/vul/emergency/operate                   | hss:vulnerability:operateEmergency          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/host-management/{host_id}/scan_status    | hss:host:getScanStatus                      | eps:enterpriseProjects:list |
| POST /v5/{project_id}/host-management/{host_id}/manual_detect | hss:host:setManualDetect                    | eps:enterpriseProjects:list |
| GET /v5/setting/account/trusted-services                      | hss::getTrustServiceStatus                  | eps:enterpriseProjects:list |
| POST /v5/setting/account/trusted-services                     | hss::enableTrustService                     | eps:enterpriseProjects:list |
| GET /v5/setting/account/admin                                 | hss::validateAdmin                          | eps:enterpriseProjects:list |
| GET /v5/setting/account/accounts                              | hss::listAccounts                           | eps:enterpriseProjects:list |
| POST /v5/setting/account/accounts                             | hss::batchAddAccounts                       | eps:enterpriseProjects:list |

| API                                                       | Action                                           | Dependencies                |
|-----------------------------------------------------------|--------------------------------------------------|-----------------------------|
| DELETE /v5/setting/account/accounts                       | hss::deleteAccount                               | eps:enterpriseProjects:list |
| GET /v5/setting/account/organization-tree                 | hss::listOrganizationTree                        | eps:enterpriseProjects:list |
| GET /v5/setting/account/delegated-accounts                | hss::listDelegatedAccounts                       | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/optional/vaults           | hss:antiransomware:listBackupVaults              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/servers                   | hss:antiransomware:listRansomwareProtectionNodes | eps:enterpriseProjects:list |
| GET /v5/{project_id}/ransomware/statistics/backups        | hss:antiransomware:getBackupsStatistics          | eps:enterpriseProjects:list |
| POST /v5/{project_id}/ransomware/backup/single_open       | hss:antiransomware:startSingleBackup             | eps:enterpriseProjects:list |
| GET /v5/{project_id}/backup/{policy_id}                   | hss:antiransomware:getBackupPolicyInfo           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/host-management/outside-group/status | hss:hostGroup:getOutsideGroupStatus              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/host-management/outside-group        | hss:hostGroup:getOutsideHostGroup                | eps:enterpriseProjects:list |
| POST /v5/{project_id}/host-management/outside-group       | hss:hostGroup:addOutsideHostGroup                | eps:enterpriseProjects:list |
| PUT /v5/{project_id}/host-management/outside-group        | hss:hostGroup:changeOutsideHostGroup             | eps:enterpriseProjects:list |



| API                                                      | Action                                  | Dependencies                |
|----------------------------------------------------------|-----------------------------------------|-----------------------------|
| GET /v5/{project_id}/image/tags                          | hss:images:listImageTag                 | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/{image_digest}/sensitive      | hss:images:listImageSensitive           | eps:enterpriseProjects:list |
| GET /v5/{project_id}/image/sensitive/filepath_whitelist  | hss:images:getFilePathWhiteDetail       | eps:enterpriseProjects:list |
| POST /v5/{project_id}/image/sensitive/filepath_whitelist | hss:images:changeFilePathWhiteDetail    | eps:enterpriseProjects:list |
| POST /v5/{project_id}/image/sensitive/operate            | hss:images:changeSensitiveInfo          | eps:enterpriseProjects:list |
| GET /v5/{project_id}/event/top-event-type                | hss:event:listTopEventType              | eps:enterpriseProjects:list |
| GET /v5/{project_id}/vulnerability/scan-policy           | hss:vulnerability:getVulScanPolicy      | -                           |
| PUT /v5/{project_id}/vulnerability/scan-policy           | hss:vulnerability:changeVulScanPolicy   | -                           |
| GET /v5/{project_id}/vulnerability/white-lists           | hss:vulnerability:listVulWhiteList      | -                           |
| GET /v5/{project_id}/vulnerability/white-list/{id}       | hss:vulnerability:getVulWhiteListDetail | -                           |
| PUT /v5/{project_id}/vulnerability/white-list/{id}       | hss:vulnerability:changeVulWhiteList    | -                           |

| API                                                                 | Action                                       | Dependencies |
|---------------------------------------------------------------------|----------------------------------------------|--------------|
| DELETE /v5/{project_id}/vulnerability/white-list/{id}               | hss:vulnerability:deleteVulWhiteList         | -            |
| POST /v5/{project_id}/vulnerability/white-list                      | hss:vulnerability:addVulWhiteList            | -            |
| GET /v5/{project_id}/vulnerability/white-list/vulnerability-options | hss:vulnerability:listVulWhiteListVulOptions | -            |
| GET /v5/{project_id}/vulnerability/scan-tasks                       | hss:vulnerability:listVulScanTask            | -            |
| GET /v5/{project_id}/vulnerability/scan-task/{task_id}/hosts        | hss:vulnerability:listVulScanTaskHost        | -            |
| PUT /v5/{project_id}/vulnerability/scan/task/{task_id}/rescan       | hss:vulnerability:rescanVulScanTask          | -            |
| GET /v5/{project_id}/vulnerability/scan/task/statistics             | hss:vulnerability:getVulScanTaskStatistics   | -            |
| GET /v5/{project_id}/vulnerability/statistics                       | hss:vulnerability:listHostVulStatistics      | -            |
| GET /v5/{project_id}/vulnerability/{host_id}/apps                   | hss:vulnerability:listVulHostApps            | -            |
| GET /v5/{project_id}/vulnerability/{host_id}/process                | hss:vulnerability:listVulHostProcess         | -            |

| API                                                                   | Action                                  | Dependencies |
|-----------------------------------------------------------------------|-----------------------------------------|--------------|
| GET /v5/{project_id}/vulnerability/handle-history                     | hss:vulnerability:listVulHandleHistory  | -            |
| GET /v5/{project_id}/vulnerability/host/hosts                         | hss:vulnerability:listVulHostHosts      | -            |
| GET /v5/{project_id}/vulnerability/host-vulnerability/vulnerabilities | hss:vulnerability:listVulHostVuls       | -            |
| GET /v5/{project_id}/vulnerability/handle/vulnerabilities             | hss:vulnerability:listVulHostHandleVuls | -            |
| GET /v5/{project_id}/image/{image_digest}/non-compliant-app           | hss:image:listImageNonCompliantApp      | -            |
| POST /v5/{project_id}/image/swr/vul/batch-export-vul                  | hss:image:batchExportSWRVulList         | -            |
| POST /v5/{project_id}/image/local/vul/batch-export-vul                | hss:image:batchExportLocalVulList       | -            |
| GET /v5/{project_id}/image/baseline/extended-weak-password            | hss:image:getExtendedWeakPassword       | -            |
| POST /v5/{project_id}/image/baseline/extended-weak-password           | hss:image:changeExtendedWeakPassword    | -            |
| GET /v5/{project_id}/image/{image_digest}/basic-image                 | hss:image:listImageBasicImage           | -            |

| API                                                                  | Action                              | Dependencies |
|----------------------------------------------------------------------|-------------------------------------|--------------|
| GET /v5/{project_id}/image/baseline/password-complexity              | hss:image:listImagePwdComplexity    | -            |
| GET /v5/{project_id}/image/baseline/weak-password-users              | hss:image:listImageWeakPwdUsers     | -            |
| GET /v5/{project_id}/image/baseline/risk-configs                     | hss:image:listImageRiskConfigs      | -            |
| GET /v5/{project_id}/image/baseline/risk-configs/{check_name}/detail | hss:image:getImageRiskConfigDetail  | -            |
| GET /v5/{project_id}/image/baseline/check-rule/detail                | hss:image:getImageCheckRuleDetail   | -            |
| GET /v5/{project_id}/image/baseline/statistic                        | hss:image:getImageBaselineStatistic | -            |
| POST /v5/{project_id}/event/white-list/userlist                      | hss:event:addSystemUserWhiteList    | -            |
| PUT /v5/{project_id}/event/white-list/userlist                       | hss:event:updateSystemUserWhiteList | -            |
| GET /v5/{project_id}/event/white-list/userlist                       | hss:event:listSystemUserWhiteList   | -            |
| DELETE /v5/{project_id}/event/white-list/userlist                    | hss:event:removeSystemUserWhiteList | -            |
| POST /v5/{project_id}/kubernetes/save-clusters                       | hss:container:saveClusters          | -            |
| GET /v5/{project_id}/kubernetes/clusters                             | hss:container:listClusterInfo       | -            |

| API                                                   | Action                            | Dependencies |
|-------------------------------------------------------|-----------------------------------|--------------|
| GET /v5/{project_id}/kubernetes/pods                  | hss:container:listPodInfo         | -            |
| GET /v5/{project_id}/kubernetes/{pod_name}/pod/detail | hss:container:showPodDetail       | -            |
| GET /v5/{project_id}/kubernetes/containers            | hss:container:listContainerInfo   | -            |
| GET /v5/{project_id}/kubernetes/container/detail      | hss:container:showContainerDetail | -            |
| GET /v5/{project_id}/kubernetes/services              | hss:container:listServiceInfo     | -            |
| GET /v5/{project_id}/kubernetes/service/detail        | hss:container:showServiceDetail   | -            |
| GET /v5/{project_id}/kubernetes/endpoints             | hss:container:listEndpointInfo    | -            |
| GET /v5/{project_id}/kubernetes/endpoint/detail       | hss:container:showEndpointDetail  | -            |
| GET /v5/{project_id}/kubernetes/deployments           | hss:container:listDeployments     | -            |
| GET /v5/{project_id}/kubernetes/statefulsets          | hss:container:listStatefulSets    | -            |
| GET /v5/{project_id}/kubernetes/daemonsets            | hss:container:listDaemonSets      | -            |

| API                                                                | Action                                   | Dependencies |
|--------------------------------------------------------------------|------------------------------------------|--------------|
| GET /v5/{project_id}/kubernetes/jobs                               | hss:container:listJobs                   | -            |
| GET /v5/{project_id}/kubernetes/cronjobs                           | hss:container:listCronJobs               | -            |
| GET /v5/{project_id}/vulnerability/statistics/affected             | hss:vulnerability:showVulAffectedStatics | -            |
| PUT /v5/{project_id}/kubernetes/{container_name}/container/isolate | hss:container:isolateK8sContainer        | -            |
| GET /v5/{project_id}/container-network/network-statistics          | hss:container:getNetworkStatistics       | -            |
| GET /v5/{project_id}/container-network/cluster-list                | hss:container:getClusters                | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/network-info   | hss:container:getClusterNetworkInfo      | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/policy-list    | hss:container:getClusterPolicyList       | -            |
| DELETE /v5/{project_id}/container-network/{cluster_id}/policy      | hss:container:deletePolicy               | -            |
| POST /v5/{project_id}/container-network/{cluster_id}/policy        | hss:container:createPolicy               | -            |

| API                                                                | Action                                           | Dependencies |
|--------------------------------------------------------------------|--------------------------------------------------|--------------|
| PUT /v5/{project_id}/container-network/{cluster_id}/policy         | hss:container:updatePolicy                       | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/policy-sync    | hss:container:syncClusterPolicyList              | -            |
| GET /v5/{project_id}/container-network/cluster-sync                | hss:container:syncClusterList                    | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/namespace-list | hss:container:getNamespaceList                   | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/node-list      | hss:container:getNodeList                        | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/node-sync      | hss:container:syncClusterNodeList                | -            |
| POST /v5/{project_id}/ransomware/protection/policy                 | hss:antiransomware:addRansomwareProtectionPolicy | -            |
| POST /v5/{project_id}/ransomware/backup/associate-policy           | hss:antiransomware:associateBackupPolicy         | -            |
| GET /v5/{project_id}/ransomware/backup/policies                    | hss:antiransomware:listBackupPolicy              | -            |

| API                                                       | Action                                       | Dependencies |
|-----------------------------------------------------------|----------------------------------------------|--------------|
| POST /v5/{project_id}/ransomware/protection/policy/deploy | hss:antiransomware:associateProtectionPolicy | -            |
| POST /v5/{project_id}/ransomware/protection/batch-open    | hss:antiransomware:batchStartProtection      | -            |
| GET /v5/{project_id}/event/att-ck                         | hss:event:getEventAttCk                      | -            |
| GET /v5/{project_id}/event/download-file                  | hss:event:downloadEventSourceFile            | -            |
| GET /v5/{project_id}/overview/security/score              | hss:overview:showSecurityScore               | -            |
| GET /v5/{project_id}/overview/security/risk/list          | hss:overview:listSecurityRisk                | -            |
| GET /v5/{project_id}/overview/quotas/host/statistics      | hss:overview:showQuotaHostStatistics         | -            |
| GET /v5/{project_id}/overview/agent/statistics            | hss:overview:showAgentStatistics             | -            |
| GET /v5/{project_id}/overview/hot/information             | hss:overview:showHotInformation              | -            |
| GET /v5/{project_id}/overview/security/risk               | hss:overview:showSecurityRisk                | -            |



| API                                                                 | Action                             | Dependencies |
|---------------------------------------------------------------------|------------------------------------|--------------|
| GET /v5/{project_id}/overview/protection/statistics                 | hss:overview:showProtectStatistics | -            |
| GET /v5/{project_id}/overview/statistics                            | hss:overview:showStatistics        | -            |
| GET /v5/{project_id}/image/swr-repository                           | hss:image:listSwrImageRepository   | -            |
| POST /v5/{project_id}/image/batch-scan                              | hss:image:batchScanSwrImage        | -            |
| GET /v5/{project_id}/image/{image_id}/vulnerabilities               | hss:image:vulnerabilities          | -            |
| GET /v5/{project_id}/image/vulnerability/{vul_id}/cve               | hss:image:listVulnerabilityCve     | -            |
| GET /v5/{project_id}/image/baseline/risk-configs/{check_name}/rules | hss:image:listImageRiskConfigRules | -            |
| POST /v5/{project_id}/image/synchronize                             | hss:image:runImageSynchronize      | -            |
| GET /v5/{project_id}/event/forensic                                 | hss:event:listEventForensic        | -            |
| GET /v5/{project_id}/event/similar-handled-events                   | hss:event:listSimilarHandledEvents | -            |
| GET /v5/{project_id}/cluster-protect/policy                         | hss:container:getPolicies          | -            |
| GET /v5/{project_id}/cluster-protect/policy/{policy_id}             | hss:container:getPolicyDetail      | -            |

| API                                                           | Action                                       | Dependencies |
|---------------------------------------------------------------|----------------------------------------------|--------------|
| GET /v5/{project_id}/cluster-protect/events                   | hss:container:getProtectEvents               | -            |
| GET /v5/{project_id}/cluster-protect/clusters                 | hss:container:getProtectClusters             | -            |
| GET /v5/{project_id}/cluster-protect/switch-mode              | hss:container:changeProtectStatus            | -            |
| GET /v5/{project_id}/cluster-protect/whiteimage               | hss:container:addWhitelma<br>ge              | -            |
| GET /v5/{project_id}/cluster-protect/default-policy           | hss:container:listDefaultPoli<br>cy          | -            |
| GET /v5/{project_id}/cluster-protect/protection-item          | hss:container:listProtectionI<br>tem         | -            |
| POST /v5/{project_id}/vulnerability/backup-statistics         | hss:vulnerability:getVulBack<br>upStatistics | -            |
| GET /v5/{project_id}/vulnerability/backup/host-vaults         | hss:vulnerability:ListVulHost<br>Vaults      | -            |
| GET /v5/{project_id}/vulnerability/backup/backups             | hss:vulnerability:ListVulHost<br>Backups     | -            |
| PUT /v5/{project_id}/vulnerability/backup/{backup_id}/restore | hss:vulnerability:RestoreVul<br>HostBackup   | -            |
| POST /v5/{project_id}/event/export                            | hss:event:exportEvent                        | -            |

| API                                              | Action                                | Dependencies |
|--------------------------------------------------|---------------------------------------|--------------|
| GET /v5/{project_id}/event/export-task/{task_id} | hss:event:queryExportTask             | -            |
| GET /v5/{project_id}/event/download/{file_id}    | hss:event:downloadEvent               | -            |
| POST /v5/{project_id}/app/policy                 | hss:ars:createAppWhitelist-Policy     | -            |
| GET /v5/{project_id}/app/policy                  | hss:ars:listAppWhitelistPolicy        | -            |
| PUT /v5/{project_id}/app/policy                  | hss:ars:changeAppWhitelist-Policy     | -            |
| DELETE /v5/{project_id}/app/policy               | hss:ars:deleteAppWhitelist-Policy     | -            |
| GET /v5/{project_id}/app/{policy_id}/detail      | hss:ars:showAppWhitelist-Policy       | -            |
| PUT /v5/{project_id}/app/host                    | hss:ars:switchAppWhitelist-PolicyHost | -            |
| POST /v5/{project_id}/app/{policy_id}/host       | hss:ars:addAppWhitelistPolicyHost     | -            |
| GET /v5/{project_id}/app/host                    | hss:ars:listAppWhitelistPolicyHost    | -            |
| DELETE /v5/{project_id}/app/{policy_id}/host     | hss:ars:deleteAppWhitelist-PolicyHost | -            |
| GET /v5/{project_id}/app/host-management/hosts   | hss:ars:listAppWhitelistHostStatus    | -            |
| GET /v5/{project_id}/app/{policy_id}/process     | hss:ars:listAppWhitelistPolicyProcess | -            |

| API                                                            | Action                                               | Dependencies |
|----------------------------------------------------------------|------------------------------------------------------|--------------|
| PUT /v5/{project_id}/app/{policy_id}/process                   | hss:ars:changeAppWhitelist-PolicyProcessStatus       | -            |
| POST /v5/{project_id}/app/{policy_id}/process                  | hss:ars:addAppWhitelistPolicyProcess                 | -            |
| GET /v5/{project_id}/app/{policy_id}/process-extend            | hss:ars:listAppWhitelistPolicyProcessExtend          | -            |
| GET /v5/{project_id}/app/{policy_id}/process/export            | hss:ars:exportAppWhitelist-PolicyProcess             | -            |
| POST /v5/{project_id}/app/{policy_id}/learn                    | hss:ars:switchAppWhitelist-PolicyLearnStatus         | -            |
| GET /v5/{project_id}/app/agent/statistics                      | hss:ars:showAppWhitelistAgentStatics                 | -            |
| GET /v5/{project_id}/app/event                                 | hss:ars:listAppWhitelistEvent                        | -            |
| DELETE /v5/{project_id}/selfbuilt/kubernetes/cluster/daemonset | hss:container:deleteSelfBuildK8sClusterDaemonsetInfo | -            |
| POST /v5/{project_id}/selfbuilt/kubernetes/cluster/daemonset   | hss:container:saveSelfBuildK8sClusterDaemonsetInfo   | -            |
| GET /v5/{project_id}/selfbuilt/kubernetes/cluster/daemonset    | hss:container:showSelfBuildK8sClusterDaemonsetInfo   | -            |
| GET /v5/{project_id}/selfbuilt/kubernetes/clusters             | hss:container:listSelfBuildK8sClusterInfo            | -            |

| API                                                       | Action                                      | Dependencies |
|-----------------------------------------------------------|---------------------------------------------|--------------|
| POST /v5/{project_id}/namespaces/{namespace}/daemonsets   | hss:container:createDaemonset               | -            |
| POST /v5/{project_id}/vulnerability/repaircmds            | hss:vulnerability:listVulRepairCmds         | -            |
| GET /v5/{project_id}/vulnerability/urgent-vulnerabilities | hss:vulnerability:listUrgentVulnerabilities | -            |
| PUT /v5/{project_id}/antivirus/task                       | hss:antivirus:switchAntivirusTask           | -            |
| GET /v5/{project_id}/antivirus/statistic                  | hss:antivirus:showAntivirusStatistic        | -            |
| GET /v5/{project_id}/image/full-scan-progress             | hss:image:showImageFullScanProgress         | -            |
| PUT /v5/{project_id}/host/operate                         | hss:host:changeHostIgnoreStatus             | -            |
| POST /v5/{project_id}/image/baseline/export               | hss:image:batchExportBaselineTask           | -            |
| POST /v5/{project_id}/image/security-report/statistic     | hss:image:showImageSecurityReportStatistic  | -            |
| POST /v5/{project_id}/vul/export                          | hss:vulnerability:exportVuls                | -            |
| GET /v5/{project_id}/export-task/{task_id}                | hss:exportTask:queryExportTask              | -            |
| GET /v5/{project_id}/download/{file_id}                   | hss:file:downloadExportedFile               | -            |

| API                                                       | Action                                   | Dependencies |
|-----------------------------------------------------------|------------------------------------------|--------------|
| GET /v5/{project_id}/image/vulnerabilities                | hss:image:listGlobalVulnerabilities      | -            |
| GET /v5/{project_id}/image/vulnerability/images           | hss:image:listVulnerabilityImages        | -            |
| GET /v5/{project_id}/setting/docker-plugin-install-script | hss:setting:getPluginInstallScript       | -            |
| GET /v5/{project_id}/setting/plugins                      | hss:setting:getPluginList                | -            |
| GET /v5/{project_id}/setting/config/auto-open-quota       | hss:setting:getAutoOpenQuotaStatus       | -            |
| PUT /v5/{project_id}/setting/config/auto-open-quota       | hss:setting:changeAutoOpenQuotaStatus    | -            |
| POST /v5/{project_id}/image/swr-vulnerability/export      | hss:image:batchExportSWRVulTask          | -            |
| POST /v5/{project_id}/image/local-vulnerability/export    | hss:image:batchExportLocalVulTask        | -            |
| GET /v5/{project_id}/setting/config/agent-auto-upgrade    | hss:setting:getAgentAutoUpgradeStatus    | -            |
| PUT /v5/{project_id}/setting/config/agent-auto-upgrade    | hss:setting:changeAgentAutoUpgradeStatus | -            |
| GET /v5/{project_id}/product/productdata/offering-infos   | hss:quota:showProductdataOfferingInfos   | -            |

| API                                                           | Action                                           | Dependencies |
|---------------------------------------------------------------|--------------------------------------------------|--------------|
| GET /v5/{project_id}/image/local/apps                         | hss:image:listLocalImageApplInfo                 | -            |
| GET /v5/{project_id}/image/local/app/vulnerabilities          | hss:image:listLocalImageApplVulnerabilities      | -            |
| GET /v5/{project_id}/ransomware/protection/status             | hss:antiransomware:getRansomwareProtectionStatus | -            |
| GET /v5/{project_id}/ransomware/protection/auto-deploy-policy | hss:antiransomware:getAutoDeployAgentList        | -            |
| PUT /v5/{project_id}/ransomware/protection/auto-deploy-policy | hss:antiransomware:updateAutoDeployAgent         | -            |
| GET /v5/{project_id}/vulnerability/individual-statistics      | hss:vulnerability:getVulIndividualStatistics     | -            |
| DELETE /v5/{project_id}/event/isolated-file                   | hss:event:deleteIsolatedFile                     | -            |
| GET /v5/{project_id}/antivirus/handle-history                 | hss:antivirus:listAntivirusHandleHistory         | -            |
| GET /v5/{project_id}/honeypot-port/host-statistics            | hss:decoyport:showStatistics                     | -            |
| GET /v5/{project_id}/honeypot-port/default-config             | hss:decoyport:showAutoBind                       | -            |

| API                                                           | Action                          | Dependencies |
|---------------------------------------------------------------|---------------------------------|--------------|
| PUT /v5/{project_id}/honeypot-port/default-config             | hss:decoyport:switchAutoBind    | -            |
| GET /v5/{project_id}/honeypot-port/host-list                  | hss:decoyport:showHostList      | -            |
| GET /v5/{project_id}/honeypot-port/policy-list                | hss:decoyport:listPolicy        | -            |
| GET /v5/{project_id}/honeypot-port/support-list               | hss:decoyport:listAvailableHost | -            |
| PUT /v5/{project_id}/honeypot-port/host-policy/{policy_id}    | hss:decoyport:switchHostPolicy  | -            |
| DELETE /v5/{project_id}/honeypot-port/host-policy/{policy_id} | hss:decoyport:deleteHostPolicy  | -            |
| POST /v5/{project_id}/honeypot-port/policy                    | hss:decoyport:createPolicy      | -            |
| PUT /v5/{project_id}/honeypot-port/policy/{policy_id}         | hss:decoyport:modifyPolicy      | -            |
| GET /v5/{project_id}/honeypot-port/policy/{policy_id}         | hss:decoyport:showPolicyDetails | -            |
| DELETE /v5/{project_id}/honeypot-port/policy/{policy_id}      | hss:decoyport:deletePolicy      | -            |



| API                                                                                    | Action                                     | Dependencies |
|----------------------------------------------------------------------------------------|--------------------------------------------|--------------|
| PUT /v5/{project_id}/honeyport-port/policy-enable/{policy_id}                          | hss:decoyport:switchPolicy                 | -            |
| GET /v5/{project_id}/export-task                                                       | hss:exportTask:queryLatestExportTaskByType | -            |
| POST /v5/{project_id}/container-network/{cluster_id}/{namespace}/security-group-policy | hss:container:createSecurityGroupPolicy    | -            |
| PUT /v5/{project_id}/container-network/{cluster_id}/{namespace}/security-group-policy  | hss:container:updateSecurityGroupPolicy    | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/security-group-policies            | hss:container:getSecurityGroupPolicyList   | -            |
| DELETE /v5/{project_id}/container-network/{cluster_id}/security-group-policy           | hss:container:deleteSecurityGroupPolicy    | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/security-group-policy-sync         | hss:container:syncSecurityGroupPolicy      | -            |
| GET /v5/{project_id}/container-network/{cluster_id}/{namespace}/workloads              | hss:container:getWorkloadList              | -            |

| API                                                    | Action                             | Dependencies |
|--------------------------------------------------------|------------------------------------|--------------|
| GET /v5/{project_id}/container-network/security-groups | hss:container:getSecurityGroupList | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-172](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for HSS.

**Table 3-172** Resource types supported by HSS

| Resource Type | URN                                                        |
|---------------|------------------------------------------------------------|
| event         | hss:<region>:<account-id>:event:<event-id>                 |
| policy        | hss:<region>:<account-id>:policy:<resource-type>/<type-id> |
| host          | hss:<region>:<account-id>:host:<host-id>                   |
| baseline      | hss:<region>:<account-id>:baseline:<type>/<check_rule_id>  |

## Conditions

HSS does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.7.10 SecMaster

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to

that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an SCP.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an SCP.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions, and you must specify all resources ("\*") in your SCP statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by SecMaster, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the **Condition** element of an SCP statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by SecMaster, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for SecMaster.

**Table 3-173** Actions supported by SecMaster (part 1)

| Action                           | Description                                                           | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:playbook:get           | Grants the permission to query playbook details.                      | read         | playbook*                   | -             | -     |
| secmaster:playbook:create        | Grants the permission to create a playbook.                           | write        | playbook*                   | -             | -     |
| secmaster:playbook:delete        | Grants the permission to delete a playbook.                           | write        | playbook*                   | -             | -     |
| secmaster:playbook:update        | Grants the permission to update a playbook.                           | write        | playbook*                   | -             | -     |
| secmaster:playbook:list          | Grants the permission to query the playbook list.                     | list         | playbook*                   | -             | -     |
| secmaster:playbook:getStatistics | Grants the permission to obtain playbook statistics.                  | read         | playbook*                   | -             | -     |
| secmaster:playbook:getMonitor    | Grants the permission to obtain the playbook running monitoring data. | read         | playbook*                   | -             | -     |
| secmaster:playbook:copyVersion   | Grants the permission to clone a playbook.                            | write        | playbook*                   | -             | -     |
| secmaster:playbook:approve       | Grants the permission to review a playbook.                           | write        | playbook*                   | -             | -     |

| Action                                 | Description                                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:playbook:listApproves        | Grants the permission to query the playbook review list.                  | list         | playbook*                   | -             | -     |
| secmaster:playbook:listInstances       | Grants the permission to query the playbook instance list.                | list         | playbook*                   | -             | -     |
| secmaster:playbook:getInstanceAuditlog | Grants the permission to query the audit log list of a playbook instance. | list         | playbook*                   | -             | -     |
| secmaster:playbook:createVersion       | Grants the permission to create a playbook version.                       | write        | playbook*                   | -             | -     |
| secmaster:playbook:getVersion          | Grants the permission to obtain a playbook version.                       | read         | playbook*                   | -             | -     |
| secmaster:playbook:deleteVersion       | Grants the permission to delete a playbook version.                       | write        | playbook*                   | -             | -     |
| secmaster:playbook:updateVersion       | Grants the permission to update a playbook version.                       | write        | playbook*                   | -             | -     |
| secmaster:playbook:listVersions        | Grants the permission to obtain the list of playbook versions.            | list         | playbook*                   | -             | -     |

| Action                                 | Description                                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:playbook:getInstance         | Grants the permission to query details about a playbook instance.          | read         | playbook *                  | -             | -     |
| secmaster:playbook:getInstanceTopology | Grants the permission to query details about a playbook instance topology. | read         | playbook *                  | -             | -     |
| secmaster:playbook:operateInstance     | Grants permissions to operate a playbook instance.                         | write        | playbook *                  | -             | -     |
| secmaster:workflow:list                | Grants the permission to query the workflow list.                          | list         | workflow *                  | -             | -     |
| secmaster:workflow:get                 | Grants the permission to obtain details about a workflow.                  | read         | workflow *                  | -             | -     |
| secmaster:workflow:delete              | Grants the permission to delete a workflow.                                | write        | workflow *                  | -             | -     |
| secmaster:workflow:create              | Grants the permission to create a workflow.                                | write        | workflow *                  | -             | -     |
| secmaster:workflow:update              | Grants the permission to update a workflow.                                | write        | workflow *                  | -             | -     |

| Action                            | Description                                                                 | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:workflow:listVersions   | Grants the permission to obtain the list of workflow versions.              | list         | workflow*                   | -             | -     |
| secmaster:workflow:getVersion     | Grants the permission to obtain details about a workflow version.           | read         | workflow*                   | -             | -     |
| secmaster:workflow:deleteVersion  | Grants the permission to delete a workflow version.                         | write        | workflow*                   | -             | -     |
| secmaster:workflow:createVersion  | Grants the permission to create a workflow version.                         | write        | workflow*                   | -             | -     |
| secmaster:workflow:updateVersion  | Grants the permission to update a workflow version.                         | write        | workflow*                   | -             | -     |
| secmaster:workflow:approveVersion | Grants the permission to review a workflow version.                         | write        | workflow*                   | -             | -     |
| secmaster:workflow:validate       | Grants the permission to verify a workflow version.                         | write        | workflow*                   | -             | -     |
| secmaster:workflow:simulate       | Grants the permission to update the debugging result of a workflow version. | write        | workflow*                   | -             | -     |

| Action                              | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias                      |
|-------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------|
| secmaster:workflow:getInstance      | Grants the permission to query the topology of a workflow instance. | read         | workflow *                  | -             | -                          |
| secmaster:workflow:operateInstance  | Grants the permission to update or create a workflow instance.      | write        | workflow *                  | -             | -                          |
| secmaster:connection:list           | Grants the permission to query the asset connection list.           | list         | connection *                | -             | -                          |
| secmaster:connection:create         | Grants the permissions to create an asset connection.               | write        | connection *                | -             | -                          |
| secmaster:connection:get            | Grants the permissions to obtain asset connection details.          | read         | connection *                | -             | -                          |
| secmaster:connection:delete         | Grants the permissions to delete an asset connection.               | write        | connection *                | -             | -                          |
| secmaster:connection:update         | Grants the permissions to update an asset connection.               | write        | connection *                | -             | -                          |
| secmaster:workspace:listWorkspace   | Grants the permission to query the workspace list.                  | list         | workspace *                 | -             | secmaster:workspace:list   |
| secmaster:workspace:createWorkspace | Grants the permission to create a workspace.                        | write        | workspace *                 | -             | secmaster:workspace:create |



| Action                              | Description                                                 | Access Level | Resource Type (*: Required) | Condition Key                          | Alias                      |
|-------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------|----------------------------|
| secmaster:workspace:updateWorkspace | Grants the permission to update a workspace.                | write        | workspace *                 | -                                      | secmaster:workspace:update |
| secmaster:workspace:getWorkspace    | Grants the permission to obtain workspace details.          | read         | workspace *                 | -                                      | secmaster:workspace:get    |
| secmaster:workspace:deleteWorkspace | Grants the permission to delete a workspace.                | write        | workspace *                 | -                                      | secmaster:workspace:delete |
| secmaster:workspace:listAgency      | Grants the permission to query the workspace agencies list. | list         | workspace *                 | -                                      | secmaster:workspace:list   |
| secmaster:workspace:createAgency    | Grants the permission to create a workspace agency.         | write        | workspace *                 | <a href="#">secmaster:TargetRegion</a> | secmaster:workspace:create |
| secmaster:workspace:updateAgency    | Grants the permission to update a workspace agency.         | write        | workspace *                 | -                                      | secmaster:workspace:update |
| secmaster:workspace:getAgency       | Grants the permission to obtain workspace agency details.   | read         | workspace *                 | -                                      | secmaster:workspace:get    |
| secmaster:workspace:deleteAgency    | Grants the permission to delete a workspace agency.         | write        | workspace *                 | -                                      | secmaster:workspace:delete |
| secmaster:task:list                 | Grants the permission to query the to-do list.              | list         | task *                      | -                                      | -                          |

| Action                        | Description                                             | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:task:create         | Grants the permission to create a to-do task.           | write        | task *                      | -             | -     |
| secmaster:task:update         | Grants the permission to update to-do tasks.            | write        | task *                      | -             | -     |
| secmaster:task:get            | Grants the permission to obtain to-do task details.     | read         | task *                      | -             | -     |
| secmaster:indicator:get       | Grants the permission to obtain indicator details.      | read         | indicator *                 | -             | -     |
| secmaster:indicator:create    | Grants the permission to create an indicator.           | write        | indicator *                 | -             | -     |
| secmaster:indicator:update    | Grants the permission to update an indicator.           | write        | indicator *                 | -             | -     |
| secmaster:indicator:delete    | Grants the permission to delete an indicator.           | write        | indicator *                 | -             | -     |
| secmaster:indicator:list      | Grants the permission to query the indicator list.      | read         | indicator *                 | -             | -     |
| secmaster:indicator:listTypes | Grants the permission to query the indicator type list. | list         | indicator *                 | -             | -     |

| Action                         | Description                                                   | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:indicator:bindLayout | Grants the permissions to bind an indicator type to a layout. | write        | indicator *                 | -             | -     |
| secmaster:alert:get            | Grants the permission to obtain alert details.                | read         | alert *                     | -             | -     |
| secmaster:alert:create         | Grants the permission to create an alert.                     | write        | alert *                     | -             | -     |
| secmaster:alert:update         | Grants the permission to update an alert.                     | write        | alert *                     | -             | -     |
| secmaster:alert:list           | Grants the permission to query the alert list.                | list         | alert *                     | -             | -     |
| secmaster:alert:delete         | Grants the permission to delete an alert.                     | write        | alert *                     | -             | -     |
| secmaster:alert:batchOrders    | Grants the permission to convert an alert to an incident.     | list         | alert *                     | -             | -     |
| secmaster:alert:listTypes      | Grants the permission to query the alert type list.           | list         | alert *                     | -             | -     |
| secmaster:alert:listCategories | Grants the permission to query the alert category list.       | list         | alert *                     | -             | -     |
| secmaster:alert:createType     | Grants the permission to create an alert type.                | write        | alert *                     | -             | -     |

| Action                       | Description                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:alert:updateType   | Grants the permission to modify an alert type.            | write        | alert *                     | -             | -     |
| secmaster:alert:deleteType   | Grants the permission to delete an alert type.            | write        | alert *                     | -             | -     |
| secmaster:alert:enableType   | Grants the permission to enable or disable an alert type. | write        | alert *                     | -             | -     |
| secmaster:alert:bindLayout   | Grants the permissions to bind an alert type to a layout. | write        | alert *                     | -             | -     |
| secmaster:incident:get       | Grants the permission to obtain incident details.         | read         | incident *                  | -             | -     |
| secmaster:incident:create    | Grants the permission to create an incident.              | write        | incident *                  | -             | -     |
| secmaster:incident:update    | Grants the permission to update an incident.              | write        | incident *                  | -             | -     |
| secmaster:incident:list      | Grants the permission to query the incident list.         | list         | incident *                  | -             | -     |
| secmaster:incident:listTypes | Grants the permission to obtain the incident type list.   | list         | incident *                  | -             | -     |

| Action                              | Description                                                  | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:incident:delete           | Grants the permission to delete an incident.                 | write        | incident *                  | -             | -     |
| secmaster:incident:listCategories   | Grants the permission to query the incident category list.   | list         | incident *                  | -             | -     |
| secmaster:incident:createType       | Grants the permission to create an incident type.            | write        | incident *                  | -             | -     |
| secmaster:incident:updateType       | Grant permission to modify an incident type.                 | write        | incident *                  | -             | -     |
| secmaster:incident:deleteType       | Grants the permission to delete an incident type.            | write        | incident *                  | -             | -     |
| secmaster:incident:enableType       | Grants the permission to enable or disable an incident type. | write        | incident *                  | -             | -     |
| secmaster:incident:bindLayout       | Grants the permissions to bind an incident type to a layout. | write        | incident *                  | -             | -     |
| secmaster:dataobject:createRelation | Grants the permission to create an object mapping.           | write        | dataobject *                | -             | -     |
| secmaster:dataobject:deleteRelation | Grants the permission to delete an object mapping.           | write        | dataobject *                | -             | -     |

| Action                              | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:dataobject:listRelation   | Grants the permission to query the object mapping list.         | list         | dataobject *                | -             | -     |
| secmaster:vulnerability:listGroup   | Grants the permission to query the vulnerability group list.    | list         | vulnerability *             | -             | -     |
| secmaster:vulnerability:getGroup    | Grants the permission to obtain vulnerability group details.    | read         | vulnerability *             | -             | -     |
| secmaster:vulnerability:exportGroup | Grants the permission to export the vulnerability group list.   | list         | vulnerability *             | -             | -     |
| secmaster:vulnerability:listType    | Grants the permission to query the vulnerability type list.     | list         | vulnerability *             | -             | -     |
| secmaster:vulnerability:bindLayout  | Grants the permission to bind a vulnerability type to a layout. | write        | vulnerability *             | -             | -     |
| secmaster:vulnerability:createType  | Grants the permission to create a vulnerability type.           | write        | vulnerability *             | -             | -     |
| secmaster:vulnerability:updateType  | Grants the permission to modify a vulnerability type.           | write        | vulnerability *             | -             | -     |

| Action                                     | Description                                                      | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:vulnerability:deleteType         | Grants the permission to delete a vulnerability type.            | write        | vulnerability *             | -             | -     |
| secmaster:vulnerability:enableType         | Grants the permission to enable or disable a vulnerability type. | write        | vulnerability *             | -             | -     |
| secmaster:subscription:deletePostPaidOrder | Grants the permission to delete a pay-per-use order.             | write        | -                           | -             | -     |
| secmaster:subscription:createPostPaidOrder | Grants the permission to create a pay-per-use order.             | write        | -                           | -             | -     |
| secmaster:subscription:createPrePaidOrder  | Grants the permission to create a yearly/monthly order.          | write        | -                           | -             | -     |
| secmaster:subscription:getVersion          | Grants the permission to view the subscribed version.            | read         | -                           | -             | -     |
| secmaster:metric:getResult                 | Grants the permission to view the metric result.                 | read         | metric *                    | -             | -     |
| secmaster:metric:listResults               | Grants the permission to list metric results.                    | list         | metric *                    | -             | -     |
| secmaster:metric:listHits                  | Grants the permission to list the hit metrics.                   | list         | metric *                    | -             | -     |

| Action                           | Description                                                   | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:agency:get             | Grants the permission to view an agency.                      | read         | -                           | -             | -     |
| secmaster:agency:create          | Grants the permission to create an agency.                    | write        | -                           | -             | -     |
| secmaster:resource:getStatistics | Grants the permission to view resource statistics.            | read         | resource *                  | -             | -     |
| secmaster:resource:list          | Grants the permission to list resources.                      | list         | resource *                  | -             | -     |
| secmaster:resource:import        | Grants the permission to import resources.                    | write        | resource *                  | -             | -     |
| secmaster:resource:getTemplate   | Grants the permission to obtain the resource import template. | read         | resource *                  | -             | -     |
| secmaster:report:list            | Grants the permission to list reports.                        | list         | report *                    | -             | -     |
| secmaster:report:get             | Grants the permission to view a report.                       | read         | report *                    | -             | -     |
| secmaster:report:create          | Grants the permission to create a report.                     | write        | report *                    | -             | -     |
| secmaster:report:update          | Grants the permission to update a report.                     | write        | report *                    | -             | -     |
| secmaster:report:delete          | Grants the permission to delete a report.                     | write        | report *                    | -             | -     |



| Action                                            | Description                                                           | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:emergencyVulnerability:updateReadStatus | Grants the permission to set the emergency vulnerability read status. | write        | emergencyVulnerability *    | -             | -     |
| secmaster:emergencyVulnerability:list             | Grants the permission to list emergency vulnerabilities.              | list         | emergencyVulnerability *    | -             | -     |
| secmaster:emergencyVulnerability:export           | Grants the permission to export emergency vulnerabilities.            | read         | emergencyVulnerability *    | -             | -     |
| secmaster:dataspace:list                          | Grants the permission to query the data space list.                   | list         | dataspace *                 | -             | -     |
| secmaster:dataspace:create                        | Grants the permission to create a data space.                         | write        | dataspace *                 | -             | -     |
| secmaster:dataspace:get                           | Grants the permission to query data space details.                    | read         | dataspace *                 | -             | -     |
| secmaster:dataspace:update                        | Grants the permission to update a data space.                         | write        | dataspace *                 | -             | -     |
| secmaster:dataspace:delete                        | Grants the permission to delete a data space.                         | write        | dataspace *                 | -             | -     |
| secmaster:pipe:list                               | Grants the permission to query the data pipeline list.                | list         | pipe *                      | -             | -     |

| Action                           | Description                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:pipe:create            | Grants the permission to create a data pipeline.          | write        | pipe *                      | -             | -     |
| secmaster:pipe:get               | Grants the permission to query data pipeline details.     | read         | pipe *                      | -             | -     |
| secmaster:pipe:update            | Grants the permission to update a data pipeline.          | write        | pipe *                      | -             | -     |
| secmaster:pipe:delete            | Grants the permission to delete a data pipeline.          | write        | pipe *                      | -             | -     |
| secmaster:pipe:getIndex          | Grants the permission to query data pipeline indexes.     | read         | pipe *                      | -             | -     |
| secmaster:pipe:updateIndex       | Grants the permission to update a data pipeline index.    | write        | pipe *                      | -             | -     |
| secmaster:pipe:getConsumption    | Grants the permission to query data pipeline consumption. | read         | pipe *                      | -             | -     |
| secmaster:pipe:createConsumption | Grants the permission to create pipeline consumption.     | write        | pipe *                      | -             | -     |
| secmaster:pipe:deleteConsumption | Grants the permission to delete pipeline consumption.     | write        | pipe *                      | -             | -     |
| secmaster:search:listLogs        | Grants the permission to query data.                      | list         | workspace *                 | -             | -     |

| Action                           | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:search:listHistograms  | Grants the permission to query the data distribution histogram. | list         | workspace *                 | -             | -     |
| secmaster:search:createAnalysis  | Grants the permission to execute security analysis.             | write        | workspace *                 | -             | -     |
| secmaster:searchCondition:list   | Grants the permission to query the list of search criteria.     | list         | searchCondition *           | -             | -     |
| secmaster:searchCondition:create | Grants the permission to create search criteria.                | write        | searchCondition *           | -             | -     |
| secmaster:searchCondition:get    | Grants the permission to query search criteria details.         | read         | searchCondition *           | -             | -     |
| secmaster:searchCondition:update | Grants the permission to update search criteria.                | write        | searchCondition *           | -             | -     |
| secmaster:searchCondition:delete | Grants the permission to delete search criteria.                | write        | searchCondition *           | -             | -     |
| secmaster:alertRule:list         | Grants the permission to query an alert model.                  | list         | alertRule *                 | -             | -     |
| secmaster:alertRule:create       | Grants the permission to create an alert model.                 | write        | alertRule *                 | -             | -     |
| secmaster:alertRule:get          | Grants the permission to query alert model details.             | read         | alertRule *                 | -             | -     |

| Action                                  | Description                                                 | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:alertRule:update              | Grants the permission to modify an alert model.             | write        | alertRule*                  | -             | -     |
| secmaster:alertRule:delete              | Grants the permission to delete an alert model.             | write        | alertRule*                  | -             | -     |
| secmaster:alertRule:enable              | Grants the permission to enable an alert model.             | write        | alertRule*                  | -             | -     |
| secmaster:alertRule:disable             | Grants the permission to disable an alert model.            | write        | alertRule*                  | -             | -     |
| secmaster:alertRule:listMetrics         | Grants the permission to query an alert model overview.     | list         | alertRule*                  | -             | -     |
| secmaster:alertRule:createSimulation    | Grants the permission to simulate an alert model.           | write        | alertRule*                  | -             | -     |
| secmaster:alertRuleTemplate:list        | Grants the permission to query an alert template.           | list         | alertRuleTemplate*          | -             | -     |
| secmaster:alertRuleTemplate:get         | Grants the permission to query alert template details.      | read         | alertRuleTemplate*          | -             | -     |
| secmaster:alertRuleTemplate:listMetrics | Grants the permission to query the alert template overview. | list         | alertRuleTemplate*          | -             | -     |

| Action                          | Description                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------|-----------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:dataclass:create      | Grants the permission to create a data class.       | write        | dataclass *                 | -             | -     |
| secmaster:dataclass:update      | Grants the permission to update a data class.       | write        | dataclass *                 | -             | -     |
| secmaster:dataclass:delete      | Grants the permission to delete a data class.       | write        | dataclass *                 | -             | -     |
| secmaster:dataclass:get         | Grants the permission to obtain data class details. | read         | dataclass *                 | -             | -     |
| secmaster:dataclass:list        | Grants the permission to query the data class list. | list         | dataclass *                 | -             | -     |
| secmaster:dataclass:createField | Grants the permission to create a field.            | write        | dataclass *                 | -             | -     |
| secmaster:dataclass:updateField | Grants the permission to update a field.            | write        | dataclass *                 | -             | -     |
| secmaster:dataclass:deleteField | Grants the permission to delete a field.            | write        | dataclass *                 | -             | -     |
| secmaster:dataclass:getField    | Grants the permission to obtain field details.      | read         | dataclass *                 | -             | -     |
| secmaster:dataclass:listFields  | Grants the permission to query the field list.      | list         | dataclass *                 | -             | -     |

| Action                          | Description                                                          | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:dataclass:getType     | Grants the permission to obtain type details.                        | read         | dataclass *                 | -             | -     |
| secmaster:dataclass:listTypes   | Grants the permission to query the type list.                        | list         | dataclass *                 | -             | -     |
| secmaster:mapping:update        | Grants the permission to update the categorical mapping status.      | write        | mapping *                   | -             | -     |
| secmaster:mapping:list          | Grant permission to search for the categorical mapping list.         | list         | mapping *                   | -             | -     |
| secmaster:mapping:getDatasource | Grants the permission to obtain the categorical mapping data source. | read         | mapping *                   | -             | -     |
| secmaster:mapping:listFunctions | Grants the permission to obtain a categorical mapping function.      | list         | mapping *                   | -             | -     |
| secmaster:mapping:delete        | Grants the permission to delete a categorical mapping.               | write        | mapping *                   | -             | -     |
| secmaster:mapping:copy          | Grants the permission to copy a categorical mapping.                 | write        | mapping *                   | -             | -     |

| Action                             | Description                                              | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:mapping:createClassifier | Grants the permission to create a category.              | write        | mapping *                   | -             | -     |
| secmaster:mapping:updateClassifier | Grants the permission to update a category.              | write        | mapping *                   | -             | -     |
| secmaster:mapping:getClassifier    | Grants the permission to obtain category information.    | read         | mapping *                   | -             | -     |
| secmaster:mapping:deleteClassifier | Grants the permission to delete a category.              | write        | mapping *                   | -             | -     |
| secmaster:mapping:createMapper     | Grants the permission to create a mapping.               | write        | mapping *                   | -             | -     |
| secmaster:mapping:updateMapper     | Grants the permission to update a mapping.               | write        | mapping *                   | -             | -     |
| secmaster:mapping:listMappers      | Grants the permission to query the mapping list.         | list         | mapping *                   | -             | -     |
| secmaster:mapping:getMapper        | Grants the permission to obtain the mapping information. | read         | mapping *                   | -             | -     |
| secmaster:mapping:deleteMapper     | Grants the permission to delete a mapping.               | write        | mapping *                   | -             | -     |
| secmaster:layout:listBusinessTypes | Grants the permission to obtain the layout type list.    | list         | layout *                    | -             | -     |

| Action                          | Description                                            | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:layout:list           | Grants the permission to query the layout list.        | list         | layout *                    | -             | -     |
| secmaster:layout:create         | Grants the permission to create a layout.              | write        | layout *                    | -             | -     |
| secmaster:layout:delete         | Grants the permission to delete a layout.              | write        | layout *                    | -             | -     |
| secmaster:layout:update         | Grants the permission to update a layout.              | write        | layout *                    | -             | -     |
| secmaster:layout:get            | Grants the permission to query a layout.               | read         | layout *                    | -             | -     |
| secmaster:layout:createTemplate | Grants the permission to save a layout as a template.  | write        | layout *                    | -             | -     |
| secmaster:layout:createField    | Grants the permission to create a layout field.        | write        | layout *                    | -             | -     |
| secmaster:layout:listFields     | Grants the permission to obtain the layout field list. | list         | layout *                    | -             | -     |
| secmaster:layout:getField       | Grants the permission to obtain layout field details.  | read         | layout *                    | -             | -     |
| secmaster:layout:updateField    | Grants the permission to update a layout field.        | write        | layout *                    | -             | -     |



| Action                        | Description                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------|-----------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:layout:deleteField  | Grants the permission to delete a layout field.     | write        | layout *                    | -             | -     |
| secmaster:layout:listWizards  | Grants the permission to obtain a page.             | list         | layout *                    | -             | -     |
| secmaster:layout:createWizard | Grants the permission to create a page.             | write        | layout *                    | -             | -     |
| secmaster:layout:getWizard    | Grants the permission to obtain page details.       | read         | layout *                    | -             | -     |
| secmaster:layout:deleteWizard | Grants the permission to delete a page.             | write        | layout *                    | -             | -     |
| secmaster:layout:updateWizard | Grants the permission to update a page.             | write        | layout *                    | -             | -     |
| secmaster:catalogue:list      | Grants the permissions to query the directory list. | list         | catalogue *                 | -             | -     |
| secmaster:catalogue:update    | Grants the permission to update a directory.        | write        | catalogue *                 | -             | -     |
| secmaster:playbook:export     | Grants the permission to export playbooks.          | read         | playbook *                  | -             | -     |
| secmaster:playbook:import     | Grants the permission to import playbooks.          | write        | playbook *                  | -             | -     |

| Action                               | Description                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:indicator:downloadTemplate | Grants the permission to download the indicator template. | read         | indicator *                 | -             | -     |
| secmaster:indicator:export           | Grants the permission to export indicators.               | read         | indicator *                 | -             | -     |
| secmaster:indicator:import           | Grants the permission to import indicators.               | write        | indicator *                 | -             | -     |
| secmaster:table:list                 | Grants the permission to query a table.                   | list         | table *                     | -             | -     |
| secmaster:table:create               | Grants the permission to create a table.                  | write        | table *                     | -             | -     |
| secmaster:table:get                  | Grants the permission to query table details.             | read         | table *                     | -             | -     |
| secmaster:table:update               | Grants the permission to modify a table.                  | write        | table *                     | -             | -     |
| secmaster:table:delete               | Grants the permission to delete a table.                  | write        | table *                     | -             | -     |
| secmaster:table:createLock           | Grants the permission to lock a table.                    | write        | table *                     | -             | -     |
| secmaster:table:deleteLock           | Grants the permission to unlock a table.                  | write        | table *                     | -             | -     |
| secmaster:table:listMetrics          | Grants the permission to query table overview.            | list         | table *                     | -             | -     |

| Action                                  | Description                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:table:updateSchema            | Grants the permission to design a table.                   | write        | table *                     | -             | -     |
| secmaster:workspace:listTags            | Grants the permission to query resource tags.              | list         | workspace *                 | -             | -     |
| secmaster:workspace:listResourcesBy-Tag | Grants the permission to query the resource instance list. | list         | workspace *                 | -             | -     |
| secmaster:workspace:listTagsForResource | Grants the permission to query resource tags.              | list         | workspace *                 | -             | -     |
| secmaster:workspace:createTags          | Grant the permission to batch add resource tags.           | write        | workspace *                 | -             | -     |
| secmaster:workspace:deleteTags          | Grants the permission to batch delete resource tags.       | write        | workspace *                 | -             | -     |
| secmaster:workspace:updateTag           | Grants the permission to update tag values.                | write        | workspace *                 | -             | -     |
| secmaster:workflow:export               | Grants the permission to export workflows.                 | read         | workflow *                  | -             | -     |
| secmaster:workflow:import               | Grants the permission to import workflows.                 | write        | workflow *                  | -             | -     |
| secmaster:alert:import                  | Grants the permission to import alerts.                    | write        | alert *                     | -             | -     |

| Action                              | Description                                                       | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:alert:export              | Grants the permission to export alerts.                           | read         | alert *                     | -             | -     |
| secmaster:alert:downloadTemplate    | Grants the permission to download an alert template.              | read         | alert *                     | -             | -     |
| secmaster:incident:import           | Grants the permission to import incidents.                        | write        | incident *                  | -             | -     |
| secmaster:incident:export           | Grants the permission to export incidents.                        | read         | incident *                  | -             | -     |
| secmaster:incident:downloadTemplate | Grants the permission to download an incident template.           | read         | incident *                  | -             | -     |
| secmaster:dataclasses:bindLayout    | Grants the permission to associate a data class type to a layout. | write        | dataclass *                 | -             | -     |
| secmaster:dataclasses:createType    | Grants the permission to create a custom data type.               | write        | dataclass *                 | -             | -     |
| secmaster:dataclasses:updateType    | Grants the permission to update a custom data type.               | write        | dataclass *                 | -             | -     |
| secmaster:dataclasses:deleteType    | Grants the permission to delete a custom data type.               | write        | dataclass *                 | -             | -     |

| Action                         | Description                                           | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:dataclass:enableType | Grants the permission to enable a data class type.    | write        | dataclass *                 | -             | -     |
| secmaster:preference:create    | Grants the permission to set user preferences.        | write        | -                           | -             | -     |
| secmaster:preference:get       | Grants the permission to obtain user preferences.     | read         | -                           | -             | -     |
| secmaster:preference:delete    | Grants the permission to delete user preferences.     | write        | -                           | -             | -     |
| secmaster:preference:update    | Grants the permission to update user preferences.     | write        | -                           | -             | -     |
| secmaster:preference:list      | Grants the permission to search for user preferences. | list         | -                           | -             | -     |
| secmaster:metric:list          | Grants the permission to obtain the metric list.      | list         | metric *                    | -             | -     |
| secmaster:metric:create        | Grants the permission to create a metric.             | write        | metric *                    | -             | -     |
| secmaster:metric:get           | Grants the permission to obtain the metric details.   | read         | metric *                    | -             | -     |
| secmaster:metric:delete        | Grants the permission to delete a metric.             | write        | metric *                    | -             | -     |

| Action                                   | Description                                                 | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:metric:update                  | Grants the permission to update a metric.                   | write        | metric *                    | -             | -     |
| secmaster:module:list                    | Grants the permission to obtain the module list.            | list         | -                           | -             | -     |
| secmaster:module:create                  | Grants the permission to create a module.                   | write        | -                           | -             | -     |
| secmaster:module:get                     | Grants the permission to obtain module details.             | read         | -                           | -             | -     |
| secmaster:module:delete                  | Grants the permission to delete a module.                   | write        | -                           | -             | -     |
| secmaster:module:update                  | Grants the permission to update a module.                   | write        | -                           | -             | -     |
| secmaster:vulnerability:downloadTemplate | Grants the permission to download a vulnerability template. | read         | vulnerability *             | -             | -     |
| secmaster:vulnerability:import           | Grants the permission to import vulnerability data.         | write        | vulnerability *             | -             | -     |
| secmaster:policy:list                    | Grants the permission to query the policy list.             | list         | policy *                    | -             | -     |
| secmaster:policy:create                  | Grants the permission to create a policy.                   | write        | policy *                    | -             | -     |

| Action                       | Description                                             | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:policy:get         | Grants the permission to query policy details.          | read         | policy *                    | -             | -     |
| secmaster:policy:update      | Grants the permission to update a policy.               | write        | policy *                    | -             | -     |
| secmaster:policy:delete      | Grants the permission to delete a policy.               | write        | policy *                    | -             | -     |
| secmaster:policy:batchDelete | Grants the permission to batch delete policies.         | write        | policy *                    | -             | -     |
| secmaster:note:list          | Grants the permission to query comments.                | list         | -                           | -             | -     |
| secmaster:note:create        | Grants the permission to create comments.               | write        | -                           | -             | -     |
| secmaster:note:delete        | Grants the permission to delete comments.               | write        | -                           | -             | -     |
| secmaster:secureScore:update | Grants the permission to update the security score.     | write        | -                           | -             | -     |
| secmaster:baseline:list      | Grants the permission to view baseline check results.   | list         | baseline *                  | -             | -     |
| secmaster:baseline:export    | Grants the permission to export baseline check results. | read         | baseline *                  | -             | -     |

| Action                              | Description                                                    | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:baseline:import           | Grants the permission to import baseline check results.        | write        | baseline *                  | -             | -     |
| secmaster:baseline:downloadTemplate | Grants the permission to download baseline check templates.    | read         | baseline *                  | -             | -     |
| secmaster:resource:get              | Grants the permission to obtain resource details.              | read         | resource *                  | -             | -     |
| secmaster:resource:getRelations     | Grants the permission to obtain resource topologies.           | read         | resource *                  | -             | -     |
| secmaster:resource:update           | Grants the permission to update resources.                     | write        | resource *                  | -             | -     |
| secmaster:resource:batchUpdate      | Grants the permission to update resources in batches.          | write        | resource *                  | -             | -     |
| secmaster:resource:batchDelete      | Grants the permission to delete resources in batches.          | write        | resource *                  | -             | -     |
| secmaster:resource:export           | Grants the permission to export resources.                     | read         | resource *                  | -             | -     |
| secmaster:resource:getSyncStatus    | Grants the permission to view resource synchronization status. | read         | resource *                  | -             | -     |



| Action                                | Description                                                                  | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:resource:sync               | Grants the permission to synchronize resources.                              | write        | resource *                  | -             | -     |
| secmaster:guide:get                   | Grants the permission to query the user guide.                               | read         | -                           | -             | -     |
| secmaster:guide:create                | Grants the permission to create a user guide.                                | write        | -                           | -             | -     |
| secmaster:shipper:list                | Grants the permission to obtain the delivery information list.               | list         | shipper *                   | -             | -     |
| secmaster:shipper:create              | Grants the permission to create data delivery.                               | write        | shipper *                   | -             | -     |
| secmaster:shipper:delete              | Grants the permission to delete delivery information.                        | write        | shipper *                   | -             | -     |
| secmaster:shipper:createAuthorization | Grants the permission to deliver authorization.                              | write        | shipper *                   | -             | -     |
| secmaster:shipper:listAuthorizations  | Grants the permission to obtain the delivery authorization information list. | list         | shipper *                   | -             | -     |
| secmaster:shipper:handleAuthorization | Grants the permission to authorize.                                          | write        | shipper *                   | -             | -     |

| Action                               | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:shipper:get                | Grants the permission to obtain the details of a delivery rule. | read         | shipper *                   | -             | -     |
| secmaster:shipper:resume             | Grants the permission to start a delivery rule.                 | write        | shipper *                   | -             | -     |
| secmaster:shipper:pause              | Grants the permission to suspend a delivery rule.               | write        | shipper *                   | -             | -     |
| secmaster:shipper:getDelegateAuth    | Grants the permission to obtain an agency.                      | read         | shipper *                   | -             | -     |
| secmaster:shipper:createDelegateAuth | Grants the permission to create an agency.                      | write        | shipper *                   | -             | -     |
| secmaster:shipper:retryAuthorization | Grants the permission to re-authorize.                          | write        | shipper *                   | -             | -     |
| secmaster:shipper:retry              | Grants the permission to re-deliver.                            | write        | shipper *                   | -             | -     |
| secmaster:adHocQuery:create          | Grants the permission to execute the analysis statement.        | write        | -                           | -             | -     |
| secmaster:adHocQuery:get             | Grants the permission to query statement results.               | read         | -                           | -             | -     |
| secmaster:adHocQuery:delete          | Grants the permission to disable query operations.              | write        | -                           | -             | -     |

| Action                              | Description                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:dataTransformation:list   | Grants the permission to query data transfer tasks.        | list         | -                           | -             | -     |
| secmaster:dataTransformation:get    | Grants the permission to query data transfer task details. | read         | -                           | -             | -     |
| secmaster:dataTransformation:enable | Grants the permission to enable a data transfer task.      | write        | -                           | -             | -     |
| secmaster:dataTransformation:create | Grants the permission to create a data transfer task.      | write        | -                           | -             | -     |
| secmaster:dataTransformation:delete | Grants the permission to delete a data transfer task.      | write        | -                           | -             | -     |
| secmaster:dataTransformation:update | Grants the permission to update a data transfer task.      | write        | -                           | -             | -     |

**Table 3-174** Actions supported by SecMaster (part 2)

| Action                                   | Description                                                    | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:dataTransformation:listMetrics | Grants the permission to query metrics of data transfer tasks. | read         | -                           | -             | -     |
| secmaster:dataTransformation:disable     | Grants the permission to disable data transfer tasks.          | write        | -                           | -             | -     |

| Action                          | Description                                             | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:analysisScript:list   | Grants the permission to query analysis scripts.        | list         | -                           | -             | -     |
| secmaster:analysisScript:create | Grants the permission to create analysis scripts.       | write        | -                           | -             | -     |
| secmaster:analysisScript:get    | Grants the permission to query analysis script details. | read         | -                           | -             | -     |
| secmaster:analysisScript:update | Grants the permission to update analysis scripts.       | write        | -                           | -             | -     |
| secmaster:analysisScript:delete | Grants the permission to delete analysis scripts.       | write        | -                           | -             | -     |
| secmaster:codeSegment:list      | Grants the permission to query code snippets.           | list         | -                           | -             | -     |
| secmaster:codeSegment:create    | Grants the permission to create code snippets.          | write        | -                           | -             | -     |
| secmaster:codeSegment:get       | Grants the permission to query code snippet details.    | read         | -                           | -             | -     |
| secmaster:codeSegment:update    | Grants the permission to update code snippets.          | write        | -                           | -             | -     |
| secmaster:codeSegment:delete    | Grants the permission to delete code snippets.          | write        | -                           | -             | -     |

| Action                              | Description                                              | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:retrieveScript:list       | Grants the permission to query retrieval scripts.        | list         | -                           | -             | -     |
| secmaster:retrieveScript:create     | Grants the permission to create retrieval scripts.       | write        | -                           | -             | -     |
| secmaster:retrieveScript:get        | Grants the permission to query retrieval script details. | read         | -                           | -             | -     |
| secmaster:retrieveScript:update     | Grants the permission to update retrieval scripts.       | write        | -                           | -             | -     |
| secmaster:retrieveScript:delete     | Grants the permission to delete retrieval scripts.       | write        | -                           | -             | -     |
| secmaster:pipe:updateSchema         | Grants the permission to modify pipeline fields.         | write        | pipe *                      | -             | -     |
| secmaster:node:create               | Grants the permission to create a node.                  | write        | -                           | -             | -     |
| secmaster:node:monitor              | Grants the permission to monitor node information.       | write        | -                           | -             | -     |
| secmaster:node:updateTaskNodeStatus | Grants the permission to modify the node task status.    | write        | -                           | -             | -     |
| secmaster:node:taskQueueDetail      | Grants the permission to query node task details.        | read         | -                           | -             | -     |

| Action                                | Description                                                                    | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:analysisScript:export       | Grants the permission to export analysis scripts.                              | read         | analysisScript *            | -             | -     |
| secmaster:analysisScript:import       | Grants the permission to import analysis scripts.                              | write        | analysisScript *            | -             | -     |
| secmaster:cloudLog:create             | Grants the permission to save cloud service log subscription configurations.   | write        | -                           | -             | -     |
| secmaster:cloudLog:delete             | Grants the permission to delete cloud service log subscription configurations. | write        | -                           | -             | -     |
| secmaster:cloudLog:list               | Grants the permission to obtain cloud service log subscription configurations. | list         | -                           | -             | -     |
| secmaster:cloudLog:listResourceConfig | Grants the permission to query asset subscription configurations.              | list         | workspace *                 | -             | -     |
| secmaster:collector:createConfig      | Grants the permission to save cloud service log subscription configurations.   | write        | -                           | -             | -     |
| secmaster:collector:listConfig        | Grants the permission to obtain cloud service log subscription configurations. | list         | -                           | -             | -     |

| Action                                     | Description                                                           | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:collectorChannel:create          | Grants the permission to create collection channels.                  | write        | collectorChannel *          | -             | -     |
| secmaster:collectorChannel:createOperation | Grants the permission to control collection channels.                 | write        | collectorChannel *          | -             | -     |
| secmaster:collectorChannel:delete          | Grants the permission to delete collection channels.                  | write        | collectorChannel *          | -             | -     |
| secmaster:collectorChannel:get             | Grants the permission to obtain collection channel details.           | read         | collectorChannel *          | -             | -     |
| secmaster:collectorChannel:list            | Grants the permission to obtain the collection channel list.          | list         | collectorChannel *          | -             | -     |
| secmaster:collectorChannel:listInstances   | Grants the permission to obtain the collection channel instance list. | list         | collectorChannel *          | -             | -     |
| secmaster:collectorChannel:listNodes       | Grants the permission to obtain the collection channel node list.     | list         | collectorChannel *          | -             | -     |
| secmaster:collectorChannel:update          | Grants the permission to update collection channels.                  | write        | collectorChannel *          | -             | -     |
| secmaster:collectorChannelGroup:create     | Grants the permission to create collection channel groups.            | write        | collectorChannelGroup *     | -             | -     |

| Action                                 | Description                                                        | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:collectorChannelGroup:delete | Grants the permission to delete collection channel groups.         | write        | collectorChannelGroup *     | -             | -     |
| secmaster:collectorChannelGroup:list   | Grants the permission to obtain the collection channel group list. | list         | collectorChannelGroup *     | -             | -     |
| secmaster:collectorChannelGroup:update | Grants the permission to update the collection channel group list. | write        | collectorChannelGroup *     | -             | -     |
| secmaster:collectorConnection:create   | Grants the permission to create collector connections.             | write        | collectorConnection *       | -             | -     |
| secmaster:collectorConnection:delete   | Grants the permission to delete collector connections.             | write        | collectorConnection *       | -             | -     |
| secmaster:collectorConnection:get      | Grants the permission to obtain collector connection details.      | read         | collectorConnection *       | -             | -     |
| secmaster:collectorConnection:list     | Grants the permission to obtain the collector connection list.     | list         | collectorConnection *       | -             | -     |
| secmaster:collectorConnection:update   | Grants the permission to update collector connections.             | write        | collectorConnection *       | -             | -     |
| secmaster:collectorNode:list           | Grants the permission to obtain the collector node list.           | list         | workspace *                 | -             | -     |



| Action                                         | Description                                                                                      | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:collectorParser:create               | Grants the permission to create a collector parser.                                              | write        | collectorParser *           | -             | -     |
| secmaster:collectorParser:delete               | Grants the permission to delete a collector parser.                                              | write        | collectorParser *           | -             | -     |
| secmaster:collectorParser:export               | Grants the permission to export a collector parser.                                              | read         | collectorParser *           | -             | -     |
| secmaster:collectorParser:get                  | Grants the permission to obtain collector parser details.                                        | read         | collectorParser *           | -             | -     |
| secmaster:collectorParser:list                 | Grants the permission to obtain the collector parser list.                                       | list         | collectorParser *           | -             | -     |
| secmaster:collectorParser:listTemplates        | Grants the permission to obtain the collector parser template list.                              | list         | collectorParser *           | -             | -     |
| secmaster:component:get                        | Grants the permission to obtain component details.                                               | read         | component *                 | -             | -     |
| secmaster:component:list                       | Grants the permission to obtain the component list.                                              | list         | component *                 | -             | -     |
| secmaster:component:listConfiguration-Versions | Grants the permission to obtain the configuration data of the historical version of a component. | list         | component *                 | -             | -     |

| Action                                   | Description                                                       | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:component:listConfigurations   | Grants the permission to obtain the component configuration list. | list         | component *                 | -             | -     |
| secmaster:component:listRunningNodes     | Grants the permission to obtain the component running node list.  | list         | component *                 | -             | -     |
| secmaster:component:listTemplates        | Grants the permission to obtain the component template list.      | list         | component *                 | -             | -     |
| secmaster:component:updateConfigurations | Grants the permission to update component configurations.         | write        | component *                 | -             | -     |
| secmaster:node:delete                    | Grants the permission to delete node information.                 | write        | node *                      | -             | -     |
| secmaster:node:list                      | Grants the permission to query the node information list.         | list         | node *                      | -             | -     |
| secmaster:node:update                    | Grants the permission to update node information.                 | write        | node *                      | -             | -     |
| secmaster:table:createConsumption        | Grants the permission to create table data consumption.           | write        | table *                     | -             | -     |
| secmaster:table:deleteConsumption        | Grants the permission to delete table data consumption.           | write        | table *                     | -             | -     |

| Action                          | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| secmaster:table:get Consumption | Grants the permission to obtain table data consumption information. | read         | table *                     | -             | -     |
| secmaster:accountAgency:list    | Grants the permission to query account management information.      | read         | accountAgency *             | -             | -     |
| secmaster:accountAgency:create  | Grants the permission to create account management.                 | write        | accountAgency *             | -             | -     |
| secmaster:accountAgency:get     | Grants the permission to obtain account management information.     | read         | accountAgency *             | -             | -     |
| secmaster:accountAgency:update  | Grants the permission to update account management information.     | write        | accountAgency *             | -             | -     |
| secmaster:accountAgency:delete  | Grants the permission to batch disassociate accounts.               | write        | accountAgency *             | -             | -     |

Each API of SecMaster usually supports one or more actions. [Table 3-175](#) lists the supported actions and dependencies.

**Table 3-175** Actions and dependencies supported by SecMaster APIs

| API                                                                        | Action                 | Dependency |
|----------------------------------------------------------------------------|------------------------|------------|
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id} | secmaster:playbook:get | -          |

| API                                                                                                  | Action                                 | Dependence |
|------------------------------------------------------------------------------------------------------|----------------------------------------|------------|
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks                                        | secmaster:playbook:create              | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}                        | secmaster:playbook:delete              | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}                           | secmaster:playbook:update              | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks                                         | secmaster:playbook:list                | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/statistics                              | secmaster:playbook:getStatistics       | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/monitor                   | secmaster:playbook:getMonitor          | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/clone   | secmaster:playbook:copyVersion         | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/approve | secmaster:playbook:approve             | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/approval                       | secmaster:playbook:listApproves        | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances                               | secmaster:playbook:listInstances       | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/auditlogs                    | secmaster:playbook:getInstanceAuditlog | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions                               | secmaster:playbook:createVersion       | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules   | secmaster:playbook:createVersionRule   | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions | secmaster:playbook:createVersionAction | -          |

| API                                                                                                             | Action                                 | Depende<br>ncy |
|-----------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------|
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}                     | secmaster:playbook:getVersion          | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}     | secmaster:playbook:getVersionRule      | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}                    | secmaster:playbook:deleteVersion       | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}    | secmaster:playbook:deleteVersionRule   | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions/{action_id} | secmaster:playbook:deleteVersionAction | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}                    | secmaster:playbook:updateVersion       | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/rules/{rule_id}     | secmaster:playbook:updateVersionRule   | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions/{action_id} | secmaster:playbook:updateVersionAction | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}/versions                             | secmaster:playbook:listVersions        | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/versions/{playbook_version_id}/actions             | secmaster:playbook:listVersionActions  | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}                            | secmaster:playbook:getInstance         | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/topology                   | secmaster:playbook:getInstanceTopology | -              |

| API                                                                                                       | Action                             | Dependence |
|-----------------------------------------------------------------------------------------------------------|------------------------------------|------------|
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/instances/{instance_id}/operation           | secmaster:playbook:operateInstance | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows                                              | secmaster:workflow:list            | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}                                | secmaster:workflow:get             | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}                             | secmaster:workflow:delete          | -          |
| GET /v1/{project_id}/workspaces<br>POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows          | secmaster:workflow:create          | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}                                | secmaster:workflow:update          | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions                       | secmaster:workflow:listVersions    | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}          | secmaster:workflow:getVersion      | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}       | secmaster:workflow:deleteVersion   | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions                      | secmaster:workflow:createVersion   | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}          | secmaster:workflow:updateVersion   | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}/approval | secmaster:workflow:approveVersion  | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/validation                    | secmaster:workflow:validate        | -          |

| API                                                                                                           | Action                             | Dependence |
|---------------------------------------------------------------------------------------------------------------|------------------------------------|------------|
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/versions/{version_id}/debug/result | secmaster:workflow:simulate        | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/instances/{instance_id}/topology                 | secmaster:workflow:getInstance     | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}/instances                         | secmaster:workflow:operateInstance | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials                                           | secmaster:connection:list          | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials                                          | secmaster:connection:create        | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}                                | secmaster:connection:get           | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}                             | secmaster:connection:delete        | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/assetcredentials/{asset_id}                                | secmaster:connection:update        | -          |
| GET /v1/{project_id}/workspaces                                                                               | secmaster:workspace:list           | -          |
| POST /v1/{project_id}/workspaces                                                                              | secmaster:workspace:create         | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}                                                                | secmaster:workspace:update         | -          |
| GET /v1/{project_id}/workspaces/v1/{project_id}/workspaces/{workspace_id}                                     | secmaster:workspace:get            | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}                                                             | secmaster:workspace:delete         | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/tasks                                                      | secmaster:task:list                | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/tasks                                                     | secmaster:task:create              | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/tasks/{task_id}                                            | secmaster:task:update              | -          |

| API                                                                             | Action                         | Dependence |
|---------------------------------------------------------------------------------|--------------------------------|------------|
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/tasks/{task_id}              | secmaster:task:get             | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}    | secmaster:indicator:get        | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators                  | secmaster:indicator:create     | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id}    | secmaster:indicator:update     | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/{indicator_id} | secmaster:indicator:delete     | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/search           | secmaster:indicator:list       | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/types             | secmaster:indicator:listTypes  | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/types/layout     | secmaster:indicator:bindLayout | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}            | secmaster:alert:get            | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts                      | secmaster:alert:create         | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/{alert_id}            | secmaster:alert:update         | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/search               | secmaster:alert:list           | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts                    | secmaster:alert:delete         | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/batch-order          | secmaster:alert:batchOrders    | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types                 | secmaster:alert:listTypes      | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/category        | secmaster:alert:listCategories | -          |



| API                                                                                    | Action                            | Dependence |
|----------------------------------------------------------------------------------------|-----------------------------------|------------|
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types                       | secmaster:alert:createType        | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/{dataclass_type_id}    | secmaster:alert:updateType        | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types                     | secmaster:alert:deleteType        | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/enable                | secmaster:alert:enableType        | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/types/layout                | secmaster:alert:bindLayout        | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}             | secmaster:incident:get            | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents                          | secmaster:incident:create         | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/{incident_id}             | secmaster:incident:update         | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/search                   | secmaster:incident:list           | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types                     | secmaster:incident:listTypes      | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/incidents                        | secmaster:incident:delete         | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/category            | secmaster:incident:listCategories | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types                    | secmaster:incident:createType     | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/{dataclass_type_id} | secmaster:incident:updateType     | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types                  | secmaster:incident:deleteType     | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/alerts/incidents/enable            | secmaster:incident:enableType     | -          |

| API                                                                                                                   | Action                              | Dependence |
|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------|------------|
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/layout                                            | secmaster:incident:bindLayout       | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}        | secmaster:dataobject:createRelation | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}      | secmaster:dataobject:deleteRelation | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/{dataclass_type}/{data_object_id}/{related_dataclass_type}/search | secmaster:dataobject:listRelation   | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/search                                              | secmaster:vulnerability:listGroup   | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/{vul_id}                                             | secmaster:vulnerability:getGroup    | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerability/export                                              | secmaster:vulnerability:exportGroup | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types                                              | secmaster:vulnerability:listType    | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/layout                                      | secmaster:vulnerability:bindLayout  | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types                                             | secmaster:vulnerability:createType  | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/{dataclass_type_id}                          | secmaster:vulnerability:updateType  | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types                                           | secmaster:vulnerability:deleteType  | -          |

| API                                                                              | Action                                     | Depende<br>ncy |
|----------------------------------------------------------------------------------|--------------------------------------------|----------------|
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/enable | secmaster:vulnerability:enableType         | -              |
| DELETE /v1/{project_id}/subscriptions/orders                                     | secmaster:subscription:deletePostPaidOrder | -              |
| POST /v1/{project_id}/subscriptions/orders                                       | secmaster:subscription:createPostPaidOrder | -              |
| POST /v1/{project_id}/subscriptions/orders/{order_id}                            | secmaster:subscription:createPrePaidOrder  | -              |
| GET /v1/{project_id}/subscriptions/version                                       | secmaster:subscription:getVersion          | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/{metric_id}/result     | secmaster:metric:getResult                 | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/results               | secmaster:metric:listResults               | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/sa/metrics/hits                  | secmaster:metric:listHits                  | -              |
| GET /v1/{project_id}/agency                                                      | secmaster:agency:get                       | -              |
| POST /v1/{project_id}/agency                                                     | secmaster:agency:create                    | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/resource-statistics               | secmaster:resource:getStatistics           | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/resources                         | secmaster:resource:list                    | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/sa/resources/import              | secmaster:resource:import                  | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/sa/resource/template              | secmaster:resource:getTemplate             | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/sa/reports                        | secmaster:report:list                      | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}            | secmaster:report:get                       | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/sa/reports                       | secmaster:report:create                    | -              |
| PUT /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}            | secmaster:report:update                    | -              |

| API                                                                              | Action                                            | Depende<br>ncy |
|----------------------------------------------------------------------------------|---------------------------------------------------|----------------|
| DELETE /v1/{project_id}/workspaces/{workspace_id}/sa/reports/{report_id}         | secmaster:report:delete                           | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/read-status     | secmaster:emergencyVulnerability:updateReadStatus | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/list             | secmaster:emergencyVulnerability:list             | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/sa/vulnerability/export           | secmaster:emergencyVulnerability:export           | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces                   | secmaster:dataspace:list                          | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces                  | secmaster:dataspace:create                        | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}    | secmaster:dataspace:get                           | -              |
| PUT /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id}    | secmaster:dataspace:update                        | -              |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/dataspaces/{dataspace_id} | secmaster:dataspace:delete                        | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes                        | secmaster:pipe:list                               | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes                       | secmaster:pipe:create                             | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}              | secmaster:pipe:get                                | -              |
| PUT /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}              | secmaster:pipe:update                             | -              |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}           | secmaster:pipe:delete                             | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/index        | secmaster:pipe:getIndex                           | -              |
| PUT /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/index        | secmaster:pipe:updateIndex                        | -              |

| API                                                                                     | Action                           | Dependence |
|-----------------------------------------------------------------------------------------|----------------------------------|------------|
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption         | secmaster:pipe:getConsumption    | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption        | secmaster:pipe:createConsumption | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/pipes/{pipe_id}/consumption      | secmaster:pipe:deleteConsumption | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/logs                        | secmaster:search:listLogs        | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/histograms                  | secmaster:search:listHistograms  | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/analysis                    | secmaster:search:createAnalysis  | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions                   | secmaster:searchCondition:list   | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions                  | secmaster:searchCondition:create | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}    | secmaster:searchCondition:get    | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id}    | secmaster:searchCondition:update | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/search/conditions/{condition_id} | secmaster:searchCondition:delete | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules                         | secmaster:alertRule:list         | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules                        | secmaster:alertRule:create       | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}               | secmaster:alertRule:get          | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/{rule_id}               | secmaster:alertRule:update       | -          |

| API                                                                                             | Action                                      | Depende<br>ncy |
|-------------------------------------------------------------------------------------------------|---------------------------------------------|----------------|
| DELETE /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules                          | secmaster:alertRule:delete                  | -              |
| POST /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules/enable                     | secmaster:alertRule:enable                  | -              |
| POST /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules/<br>disable                | secmaster:alertRule:disabl<br>e             | -              |
| GET /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules/<br>metrics                 | secmaster:alertRule:listMe<br>trics         | -              |
| POST /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules/<br>simulation             | secmaster:alertRule:create<br>Simulation    | -              |
| GET /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules/<br>templates               | secmaster:alertRuleTempla<br>te:list        | -              |
| GET /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules/<br>templates/{template_id} | secmaster:alertRuleTempla<br>te:get         | -              |
| GET /v1/{project_id}/workspaces/<br>{workspace_id}/siem/alert-rules/<br>templates/metrics       | secmaster:alertRuleTempla<br>te:listMetrics | -              |
| POST /v1/{project_id}/workspaces/<br>{workspace_id}/soc/dataclasses                             | secmaster:dataclass:create                  | -              |
| PUT /v1/{project_id}/workspaces/<br>{workspace_id}/soc/dataclasses/<br>{dataclass_id}           | secmaster:dataclass:updat<br>e              | -              |
| DELETE /v1/{project_id}/workspaces/<br>{workspace_id}/soc/dataclasses/<br>{dataclass_id}        | secmaster:dataclass:delete                  | -              |
| GET /v1/{project_id}/workspaces/<br>{workspace_id}/soc/dataclasses/<br>{dataclass_id}           | secmaster:dataclass:get                     | -              |
| GET /v1/{project_id}/workspaces/<br>{workspace_id}/soc/dataclasses                              | secmaster:dataclass:list                    | -              |
| POST /v1/{project_id}/workspaces/<br>{workspace_id}/soc/dataclasses/<br>{dataclass_id}/fields   | secmaster:dataclass:create<br>Field         | -              |

| API                                                                                                     | Action                             | Dependence |
|---------------------------------------------------------------------------------------------------------|------------------------------------|------------|
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields/{field_id}         | secmaster:dataclass:updateField    | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields                 | secmaster:dataclass:deleteField    | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields/{field_id}         | secmaster:dataclass:getField       | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields                    | secmaster:dataclass:listFields     | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/types/{dataclass_type_id} | secmaster:dataclass:getType        | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/types                     | secmaster:dataclass:listTypes      | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}/status                         | secmaster:mapping:update           | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/search                                     | secmaster:mapping:list             | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/data-source                                 | secmaster:mapping:getDataSource    | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/functions                                   | secmaster:mapping:listFunctions    | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}                             | secmaster:mapping:delete           | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/{mapping_id}/clone                          | secmaster:mapping:copy             | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers                                | secmaster:mapping:createClassifier | -          |

| API                                                                                        | Action                             | Dependence |
|--------------------------------------------------------------------------------------------|------------------------------------|------------|
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}    | secmaster:mapping:updateClassifier | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id}    | secmaster:mapping:getClassifier    | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/classifiers/{classifier_id} | secmaster:mapping:deleteClassifier | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers                       | secmaster:mapping:createMapper     | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}            | secmaster:mapping:updateMapper     | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/search                | secmaster:mapping:listMappers      | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}           | secmaster:mapping:getMapper        | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/mappings/mappers/{mapper_id}         | secmaster:mapping:deleteMapper     | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/business-type                   | secmaster:layout:listBusinessTypes | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/search                         | secmaster:layout:list              | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts                                | secmaster:layout:create            | -          |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts                              | secmaster:layout:delete            | -          |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}                     | secmaster:layout:update            | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}                     | secmaster:layout:get               | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/template                       | secmaster:layout:createTemplate    | -          |



| API                                                                                                                                           | Action                        | Depende<br>ncy |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------------|
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields                                                                | secmaster:layout:createField  | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields                                                                 | secmaster:layout:listFields   | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields/{field_id}                                                      | secmaster:layout:getField     | -              |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields/{field_id}                                                      | secmaster:layout:updateField  | -              |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/fields                                                              | secmaster:layout:deleteField  | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/wizards                                                                | secmaster:layout:listWizards  | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/{layout_id}/wizards                                                               | secmaster:layout:createWizard | -              |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards/{wizard_id};/v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards | secmaster:layout:getWizard    | -              |
| DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards/{wizard_id}                                                             | secmaster:layout:deleteWizard | -              |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/layouts/wizards                                                                            | secmaster:layout:updateWizard | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/catalogues/search;/v1/{project_id}/workspaces/{workspace_id}/soc/catalogues               | secmaster:catalogue:list      | -              |
| PUT /v1/{project_id}/workspaces/{workspace_id}/soc/catalogues/{catalogue_id}                                                                  | secmaster:catalogue:update    | -              |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/export                                                                          | secmaster:playbook:export     | -              |

| API                                                                             | Action                               | Dependence |
|---------------------------------------------------------------------------------|--------------------------------------|------------|
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/import            | secmaster:playbook:import            | -          |
| GET /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/template/download | secmaster:indicator:downloadTemplate | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/export           | secmaster:indicator:export           | -          |
| POST /v1/{project_id}/workspaces/{workspace_id}/soc/indicators/import           | secmaster:indicator:import           | -          |
| GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables                      | secmaster:table:list                 | -          |
| -POST /v2/{project_id}/workspaces/{workspace_id}/siem/tables                    | secmaster:table:create               | -          |
| GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}           | secmaster:table:get                  | -          |
| PUT /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}           | secmaster:table:update               | -          |
| DELETE /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}        | secmaster:table:delete               | -          |
| POST /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/lock     | secmaster:table:createLock           | -          |
| DELETE /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/lock   | secmaster:table:deleteLock           | -          |
| GET /v2/{project_id}/workspaces/{workspace_id}/siem/tables/metrics              | secmaster:table:listMetrics          | -          |
| PUT /v2/{project_id}/workspaces/{workspace_id}/siem/tables/{table_id}/schema    | secmaster:table:updateSchema         | -          |

## Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action, the resource URN must be specified in the SCP statements using that action, and the SCP applies only to resources of this type. If no resource type is specified, the **Resource** element is marked with an asterisk (\*) and the SCP applies to all resources. You can also set condition keys in an SCP to define resource types.

The following table lists the resource types that you can define in SCP statements for SecMaster.

**Table 3-176** Resource types supported by SecMaster

| Resource Type          | URN                                                                                                |
|------------------------|----------------------------------------------------------------------------------------------------|
| workspace              | secmaster:<region>:<account-id>:workspace:<workspace-id>                                           |
| playbook               | secmaster:<region>:<account-id>:playbook:<workspace-id>/<playbook-id>                              |
| workflow               | secmaster:<region>:<account-id>:workflow:<workspace-id>/<workflow-id>                              |
| connection             | secmaster:<region>:<account-id>:connection:<workspace-id>/<connection-id>                          |
| task                   | secmaster:<region>:<account-id>:task:<workspace-id>/<task-id>                                      |
| indicator              | secmaster:<region>:<account-id>:indicator:<workspace-id>/<indicator-id>                            |
| alert                  | secmaster:<region>:<account-id>:alert:<workspace-id>/<alert-id>                                    |
| incident               | secmaster:<region>:<account-id>:incident:<workspace-id>/<incident-id>                              |
| dataobject             | secmaster:<region>:<account-id>:dataobject:<workspace-id>/<dataobject-id>                          |
| metric                 | secmaster:<region>:<account-id>:metric:<workspace-id>/<metric-id>                                  |
| resource               | secmaster:<region>:<account-id>:resource:<workspace-id>/<resource-id>                              |
| report                 | secmaster:<region>:<account-id>:report:<workspace-id>/<report-id>                                  |
| emergencyVulnerability | secmaster:<region>:<account-id>:emergencyVulnerability:<workspace-id>/<emergency-vulnerability-id> |
| dataspace              | secmaster:<region>:<account-id>:dataspace:<workspace-id>/<dataspace-id>                            |
| pipe                   | secmaster:<region>:<account-id>:pipe:<workspace-id>/<pipe-id>                                      |
| alertRule              | secmaster:<region>:<account-id>:alertRule:<workspace-id>/<alertRule-id>                            |
| vulnerability          | secmaster:<region>:<account-id>:vulnerability:<workspace-id>/<vulnerability-id>                    |

| Resource Type         | URN                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------|
| alertRuleTemplate     | secmaster:<region>:<account-id>:alertRuleTemplate:<workspace-id>/<alertRuleTemplate-id>         |
| searchCondition       | secmaster:<region>:<account-id>:searchCondition:<workspace-id>/<searchCondition-id>             |
| dataclass             | secmaster:<region>:<account-id>:dataclass:<workspace-id>/<dataclass-id>                         |
| mapping               | secmaster:<region>:<account-id>:mapping:<workspace-id>/<mapping-id>                             |
| layout                | secmaster:<region>:<account-id>:layout:<workspace-id>/<layout-id>                               |
| catalogue             | secmaster:<region>:<account-id>:catalogue:<workspace-id>/<catalogue-id>                         |
| table                 | secmaster:<region>:<account-id>:table:<workspace-id>/<table-id>                                 |
| policy                | secmaster:<region>:<account-id>:policy:<workspace-id>/<policy-id>                               |
| baseline              | secmaster:<region>:<account-id>:baseline:<workspace-id>/<baseline-id>                           |
| shipper               | secmaster:<region>:<account-id>:shipper:<workspace-id>/<shipper-id>                             |
| analysisScript        | secmaster:<region>:<account-id>:analysisScript:<workspace-id>/<analysisScript-id>               |
| collectorChannel      | secmaster:<region>:<account-id>:collectorChannel:<workspace-id>/<collectorChannel-id>           |
| collectorChannelGroup | secmaster:<region>:<account-id>:collectorChannelGroup:<workspace-id>/<collectorChannelGroup-id> |
| collectorConnection   | secmaster:<region>:<account-id>:collectorConnection:<workspace-id>/<collectorConnection-id>     |
| collectorParser       | secmaster:<region>:<account-id>:collectorParser:<workspace-id>/<collectorParser-id>             |
| component             | secmaster:<region>:<account-id>:component:<workspace-id>/<component-id>                         |
| node                  | secmaster:<region>:<account-id>:node:<workspace-id>/<node-id>                                   |
| accountAgency         | secmaster:<region>:<account-id>:accountAgency:<accountAgency-id>                                |

## Conditions

### Condition Key

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- Condition keys are the key values in the Condition element of an identity policy statement. Condition keys are classified into global condition keys and service-specific condition keys based on the application scope.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, secmaster:) apply only to operations of the service. For details, see [Table 3-177](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, a condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by SecMaster

The following table lists the condition keys that you can define in identity policies for SecMaster. You can include these condition keys to specify conditions for when your identity policy is in effect.

SecMaster does not support service-specific condition keys in SCP statements.

**Table 3-177** Service-specific condition keys supported by SecMaster

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Important Notes                                                                                                                                                                                                                                                |
|--------------------------------|--------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| secmaster:TargetRegion         | String | Multivalued                   | Only the action secmaster:workspace:createAgency supports this service-level condition key. The target region specified by the condition key <b>secmaster:TargetRegion</b> are filtered based on the region attribute of the managed workspace in the request. |

### Condition Key Examples

- secmaster:TargetRegion

Example: Workspace agencies cannot be created in the region with ID 1.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "secmaster:workspace:createAgency"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "secmaster:TargetRegion": [
            "region_id_1"
          ]
        }
      }
    }
  ]
}
```

## 3.8 AI

### 3.8.1 ModelArts

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are

available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by modelarts, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by modelarts, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for modelarts.

**Table 3-178** Actions supported by modelarts

| Action                    | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                    | Alias |
|---------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| modelarts:notebook:list   | Grants permission to list the development environment instances.  | List         | notebook *                  | -                                                                                                                                                                                                                                                                                | -     |
|                           |                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                           |       |
| modelarts:notebook:create | Grants permission to create a development environment instance.   | Write        | notebook *                  | -                                                                                                                                                                                                                                                                                | -     |
|                           |                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">modelarts:poolType</a></li> <li>• <a href="#">modelarts:poolId</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> |       |
| modelarts:notebook:get    | Grants permission to get development environment instance detail. | Read         | notebook *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                                                                    | -     |
|                           |                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">modelarts:poolType</a></li> <li>• <a href="#">modelarts:poolId</a></li> </ul>                                                                                              |       |
| modelarts:notebook:update | Grants permission to update a development environment instance.   | Write        | notebook *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                                                                    | -     |



| Action                    | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                       | Alias |
|---------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                           |                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">modelarts:poolType</a></li> <li>• <a href="#">modelarts:poolId</a></li> </ul> |       |
| modelarts:notebook:delete | Grants permission to delete a development environment instance.             | Write        | notebook *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                       | -     |
|                           |                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">modelarts:poolType</a></li> <li>• <a href="#">modelarts:poolId</a></li> </ul> |       |
| modelarts:image:create    | Grants permission to save a image for the development environment instance. | Write        | image *                     | -                                                                                                                                                                                   | -     |
|                           |                                                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                               |       |
| modelarts:notebook:start  | Grants permission to start a development environment instance.              | Write        | notebook *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                       | -     |
|                           |                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">modelarts:poolType</a></li> <li>• <a href="#">modelarts:poolId</a></li> </ul> |       |
| modelarts:notebook:stop   | Grants permission to stop a development environment instance.               | Write        | notebook *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                       | -     |

| Action                                 | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                 | Alias |
|----------------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------|
|                                        |                                                                                   |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>modelarts:poolType</li> <li>modelarts:poolId</li> </ul> |       |
| modelarts:image:list                   | Grants permission to list the images.                                             | List         | image *                     | -                                                                                                                             | -     |
|                                        |                                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                         |       |
| modelarts:image:register               | Grants permission to register a image.                                            | Write        | image *                     | -                                                                                                                             | -     |
|                                        |                                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                         |       |
| modelarts:image:get                    | Grants permission to get a image detail.                                          | Read         | image *                     | -                                                                                                                             | -     |
|                                        |                                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                         |       |
| modelarts:image:delete                 | Grants permission to delete a image.                                              | Write        | image *                     | -                                                                                                                             | -     |
|                                        |                                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                         |       |
| modelarts:notebook:listMountedStorages | Grants permission to list mounted storages of a development environment instance. | List         | notebook *                  | -                                                                                                                             | -     |
|                                        |                                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                         |       |
| modelarts:notebook:mountStorage        | Grants permission to mount a storage for the development environment instance.    | Write        | notebook *                  | -                                                                                                                             | -     |
|                                        |                                                                                   |              | -                           | g:EnterpriseProjectId                                                                                                         |       |

| Action                               | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|--------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| modelarts:notebook:getMountedStorage | Grants permission to get a storage detail for the development environment instance. | Read         | notebook *                  | -                                                                                                                                 | -     |
|                                      |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             |       |
| modelarts:notebook:umountStorage     | Grants permission to umount a storage for the development environment instance.     | Write        | notebook *                  | -                                                                                                                                 | -     |
|                                      |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             |       |
| modelarts:notebook:updateStopPolicy  | Grants permission to update a stop rule for the development environment instance.   | Write        | notebook *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                      |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             |       |
| modelarts:model:create               | Grants permission to import a model.                                                | Write        | model *                     | -                                                                                                                                 | -     |
|                                      |                                                                                     |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| modelarts:model:list                 | Grants permission to query the model list.                                          | List         | model *                     | -                                                                                                                                 | -     |
|                                      |                                                                                     |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| modelarts:model:delete               | Grants permission to delete the model.                                              | Write        | model *                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |

| Action                       | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|------------------------------|---------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| modelarts:model:get          | Grants permission to query the details about a model.         | Read         | model *                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| modelarts:service:create     | Grants permission to deploy a model service.                  | Write        | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | -     |
| modelarts:service:list       | Grants permission to query the model service list.            | List         | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | -     |
| modelarts:service:get        | Grants permission to query the details about a model service. | Read         | service *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| modelarts:service:update     | Grants permission to update a model service.                  | Write        | service *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| modelarts:service:delete     | Grants permission to delete a model service.                  | Write        | service *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| modelarts:service:getMonitor | Grants permission to query service monitoring information.    | Read         | service *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| modelarts:service:getLogs    | Grants permission to query service update logs.               | Read         | service *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |

| Action                       | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                   | Alias |
|------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| modelarts:service:getEvents  | Grants permission to query service event logs.             | Read         | service *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                   | -     |
| modelarts:trainJob:create    | Grants permission to create a training job.                | Write        | trainJob *                  | -                                                                                                                                                                                                                               | -     |
|                              |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">modelarts:poolType</a></li> <li>• <a href="#">modelarts:poolId</a></li> </ul> |       |
| modelarts:aiAlgorithm:create | Grants permission to create ai algorithm.                  | Write        | aiAlgorithm *               | -                                                                                                                                                                                                                               | -     |
| modelarts:aiAlgorithm:list   | Grants permission to query the ai algorithm list.          | List         | -                           | -                                                                                                                                                                                                                               | -     |
| modelarts:aiAlgorithm:get    | Grants permission to query the details about ai algorithm. | Read         | aiAlgorithm *               | -                                                                                                                                                                                                                               | -     |
| modelarts:aiAlgorithm:update | Grants permission to update ai algorithm.                  | Write        | aiAlgorithm *               | -                                                                                                                                                                                                                               | -     |
| modelarts:aiAlgorithm:delete | Grants permission to delete ai algorithm.                  | Write        | aiAlgorithm *               | -                                                                                                                                                                                                                               | -     |
| modelarts:trainJob:get       | Grants permission to view a training job.                  | Read         | trainJob *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                   | -     |

| Action                        | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                  | Alias |
|-------------------------------|----------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------|-------|
|                               |                                                                |              | -                           | <ul style="list-style-type: none"> <li>modelarts:poolType</li> <li>modelarts:poolId</li> </ul> |       |
| modelarts:trainJob:update     | Grants permission to modify the description of a training job. | Write        | trainJob *                  | g:ResourceTag/<tag-key>                                                                        | -     |
|                               |                                                                |              | -                           | <ul style="list-style-type: none"> <li>modelarts:poolType</li> <li>modelarts:poolId</li> </ul> |       |
| modelarts:trainJob:delete     | Grants permission to delete a training job.                    | Write        | trainJob *                  | g:ResourceTag/<tag-key>                                                                        | -     |
|                               |                                                                |              | -                           | <ul style="list-style-type: none"> <li>modelarts:poolType</li> <li>modelarts:poolId</li> </ul> |       |
| modelarts:trainJob:logview    | Grants permission to preview training job log.                 | Read         | trainJob *                  | -                                                                                              | -     |
| modelarts:trainJob:logExport  | Grants permission to export training job log.                  | Write        | trainJob *                  | -                                                                                              | -     |
| modelarts:trainJob:getmetrics | Grants permission to show training job metrics.                | Read         | trainJob *                  | -                                                                                              | -     |
| modelarts:trainJob:list       | Grants permission to query the training job list.              | List         | -                           | -                                                                                              | -     |

| Action                             | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| modelarts:trainJob:setHighPriority | Grants permission to set the highest priority for a training job. | Write        | -                           | -                                                                                                                                                                                      | -     |
| modelarts:trainJob:exec            | Grants permission to access training jobs through CloudShell.     | Write        | -                           | -                                                                                                                                                                                      | -     |
| modelarts:network:create           | Grants permission to create a network.                            | Write        | network *                   | -                                                                                                                                                                                      | -     |
|                                    |                                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| modelarts:network:get              | Grants permission to view a network.                              | Read         | network *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | -     |
|                                    |                                                                   |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:workflow:list            | Grants permission to query the workflow list.                     | List         | -                           | -                                                                                                                                                                                      | -     |
| modelarts:workflow:create          | Grants permission to create a workflow.                           | Write        | workflow *                  | -                                                                                                                                                                                      | -     |
| modelarts:workflow:delete          | Grants permission to delete a workflow.                           | Write        | workflow *                  | -                                                                                                                                                                                      | -     |

| Action                           | Description                                               | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| modelarts:workflow:get           | Grants permission to view a workflow.                     | Read         | workflow *                  | -             | -     |
| modelarts:workflow:update        | Grants permission to update a workflow.                   | Write        | workflow *                  | -             | -     |
| modelarts:workflow:execute       | Grants permission to execute a workflow.                  | Write        | workflow *                  | -             | -     |
| modelarts:workspace:get          | Grants permission to query the details about a workspace. | Read         | workspace *                 | -             | -     |
| modelarts:workspace:update       | Grants permission to modify a workspace.                  | Write        | workspace *                 | -             | -     |
| modelarts:workspace:delete       | Grants permission to delete a workspace.                  | Write        | workspace *                 | -             | -     |
| modelarts:workspace:getQuotas    | Grants permission to query the workspace quota.           | Read         | workspace *                 | -             | -     |
| modelarts:workspace:updateQuotas | Grants permission to modify the workspace quota.          | Write        | workspace *                 | -             | -     |
| modelarts:dataset:list           | Grants permission to query the dataset list.              | List         | dataset *                   | -             | -     |



| Action                           | Description                                              | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| modelarts:dataset:create         | Grants permission to create a dataset.                   | Write        | dataset *                   | -             | -     |
| modelarts:workspace:list         | Query the workspace list                                 | List         | -                           | -             | -     |
| modelarts:workspace:create       | Grants permission to create a workspace.                 | Write        | workspace *                 | -             | -     |
| modelarts:dataset:get            | Grants permission to query the details about a dataset.  | Read         | dataset *                   | -             | -     |
| modelarts:dataset:update         | Grants permission to update a dataset.                   | Write        | dataset *                   | -             | -     |
| modelarts:dataset:delete         | Grants permission to delete a dataset.                   | Write        | dataset *                   | -             | -     |
| modelarts:dataset:publishVersion | Grants permission to release a new version of a dataset. | Write        | dataset *                   | -             | -     |
| modelarts:dataset:deleteVersion  | Grants permission to delete a dataset version.           | Write        | dataset *                   | -             | -     |
| modelarts:dataAnnotation:list    | Grants permission to query the labels of a dataset.      | List         | dataAnnotation *            | -             | -     |

| Action                          | Description                                                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------|--------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| modelarts:dataAnnotation:upload | Grants permission to upload the files to be labeled in batches, such as images, sound files, and text. | Write        | dataAnnotation *            | -             | -     |
| modelarts:dataAnnotation:delete | Grants permission to delete the labels of a dataset in batches.                                        | Write        | dataAnnotation *            | -             | -     |
| modelarts:dataAnnotation:get    | Grants permission to query the labeling information about a dataset.                                   | Read         | dataAnnotation *            | -             | -     |
| modelarts:dataAnnotation:create | Grants permission to create labels for a dataset in batches.                                           | Write        | dataAnnotation *            | -             | -     |
| modelarts:dataAnnotation:update | Grants permission to modify the labels of a dataset in batches.                                        | Write        | dataAnnotation *            | -             | -     |
| modelarts:dataset:import        | Grants permission to create import task.                                                               | Write        | dataset *                   | -             | -     |
| modelarts:dataset:export        | Grants permission to create export task.                                                               | Write        | dataset *                   | -             | -     |

| Action                   | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|--------------------------|--------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| modelarts:network:list   | Grants permission to query the network list.           | List         | network *                   | -                                                                                                                                                                                      |       |
|                          |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> |       |
| modelarts:network:delete | Grants permission to delete a network.                 | Write        | network *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | -     |
|                          |                                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:network:update | Grants permission to update a network.                 | Write        | network *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | -     |
|                          |                                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:pool:get       | Grants permission to view a dedicated resource pool.   | Read         | pool *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | -     |
|                          |                                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:pool:update    | Grants permission to update a dedicated resource pool. | Write        | pool *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | -     |
|                          |                                                        |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:pool:create    | Grants permission to create a dedicated resource pool. | Write        | pool *                      | -                                                                                                                                                                                      |       |
|                          |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |

| Action                     | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|----------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| modelarts:pool:list        | Grants permission to query the dedicated resource pools.                     | List         | pool *                      | -                                                                                                                                                                                      | -     |
|                            |                                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| modelarts:pool:delete      | Grants permission to delete a dedicated resource pool.                       | Write        | pool *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | -     |
|                            |                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:devserver:list   | Grants permission to query the details of all DevServer instances by tenant. | List         | devserver *                 | -                                                                                                                                                                                      | -     |
|                            |                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:devserver:create | Grants permission to create a DevServer instance.                            | Write        | devserver *                 | -                                                                                                                                                                                      | -     |
|                            |                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:devserver:get    | Grants permission to query DevServer instance detail information.            | Read         | devserver *                 | -                                                                                                                                                                                      | -     |
|                            |                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| modelarts:devserver:delete | Grants permission to delete a DevServer instance.                            | Write        | devserver *                 | -                                                                                                                                                                                      | -     |
|                            |                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |

| Action                          | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|---------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| modelarts:devserver:sync        | Grants permission to synchronize the status of all DevServer instances of the user. | Write        | devserver *                 | -                                     | -     |
|                                 |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:start       | Grants permission to start a DevServer instance.                                    | Write        | devserver *                 | -                                     | -     |
|                                 |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:stop        | Grants permission to stop a DevServer instance.                                     | Write        | devserver *                 | -                                     | -     |
|                                 |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:changeOS    | Grants permission to change a DevServer instance OS.                                | Write        | devserver *                 | -                                     | -     |
|                                 |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:reinstallOS | Grants permission to reinstall a DevServer instance OS.                             | Write        | devserver *                 | -                                     | -     |
|                                 |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:reboot      | Grants permission to reboot a DevServer instance.                                   | Write        | devserver *                 | -                                     | -     |
|                                 |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:createTags  | Grants permission to add a DevServer instance tags.                                 | Write        | devserver *                 | -                                     | -     |
|                                 |                                                                                     |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |

| Action                           | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| modelarts:devserver:deleteTags   | Grants permission to delete a DevServer instance tags.          | Write        | devserver *                 | -                                     | -     |
|                                  |                                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:queryTags    | Grants permission to query DevServer instance tags information. | Read         | devserver *                 | -                                     | -     |
|                                  |                                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:image:listGroup        | Grants permission to list the image groups.                     | List         | image *                     | -                                     | -     |
| modelarts:devserver:bindPublicIP | Grant the permission to bind an EIP to the DevServer.           | Write        | devserver *                 | -                                     | -     |
|                                  |                                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| modelarts:devserver:listPublicIP | Grant the permission to query the EIP bound to the DevServer.   | Read         | devserver *                 | -                                     | -     |
|                                  |                                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |

Each API of modelarts usually supports one or more actions. [Table 3-179](#) lists the supported actions and dependencies.

**Table 3-179** Actions and dependencies supported by modelarts APIs

| API                             | Action                    | Dependency |
|---------------------------------|---------------------------|------------|
| GET /v1/{project_id}/notebooks  | modelarts:notebook:list   | -          |
| POST /v1/{project_id}/notebooks | modelarts:notebook:create | -          |

| API                                                   | Action                                 | Dependency |
|-------------------------------------------------------|----------------------------------------|------------|
| GET /v1/{project_id}/notebooks/{id}                   | modelarts:notebook:get                 | -          |
| PUT /v1/{project_id}/notebooks/{id}                   | modelarts:notebook:update              | -          |
| DELETE /v1/{project_id}/notebooks/{id}                | modelarts:notebook:delete              | -          |
| POST /v1/{project_id}/notebooks/{id}/create-image     | modelarts:image:create                 | -          |
| POST /v1/{project_id}/notebooks/{id}/start            | modelarts:notebook:start               | -          |
| POST /v1/{project_id}/notebooks/{id}/stop             | modelarts:notebook:stop                | -          |
| GET /v1/{project_id}/images                           | modelarts:image:list                   | -          |
| POST /v1/{project_id}/images                          | modelarts:image:register               | -          |
| GET /v1/{project_id}/images/{id}                      | modelarts:image:get                    | -          |
| DELETE /v1/{project_id}/images/{id}                   | modelarts:image:delete                 | -          |
| GET /v1/{project_id}/notebooks/{instance_id}/storage  | modelarts:notebook:listMountedStorages | -          |
| POST /v1/{project_id}/notebooks/{instance_id}/storage | modelarts:notebook:mountStorage        | -          |

| API                                                                  | Action                               | Dependency |
|----------------------------------------------------------------------|--------------------------------------|------------|
| GET /v1/{project_id}/notebooks/{instance_id}/storage/{storage_id}    | modelarts:notebook:getMountedStorage | -          |
| DELETE /v1/{project_id}/notebooks/{instance_id}/storage/{storage_id} | modelarts:notebook:umountStorage     | -          |
| PATCH /v1/{project_id}/notebooks/{id}/lease                          | modelarts:notebook:updateStopPolicy  | -          |
| GET /v1/{project_id}/models                                          | modelarts:model:list                 | -          |
| POST /v1/{project_id}/models                                         | modelarts:model:create               | -          |
| GET /v1/{project_id}/models/{model_id}                               | modelarts:model:get                  | -          |
| DELETE /v1/{project_id}/models/{model_id}                            | modelarts:model:delete               | -          |
| GET /v1/{project_id}/services/{service_id}/monitor                   | modelarts:service:getMonitor         | -          |
| GET /v1/{project_id}/services                                        | modelarts:service:list               | -          |
| POST /v2/{project_id}/training-jobs                                  | modelarts:trainJob:create            | -          |
| POST /v2/{project_id}/algorithms                                     | modelarts:aiAlgorithm:create         | -          |
| GET /v2/{project_id}/algorithms                                      | modelarts:aiAlgorithm:list           | -          |



| API                                                                                               | Action                       | Dependency |
|---------------------------------------------------------------------------------------------------|------------------------------|------------|
| GET /v2/<br>{project_id}/<br>algorithms/<br>{algorithm_id}                                        | modelarts:aiAlgorithm:get    | -          |
| PUT /v2/<br>{project_id}/<br>algorithms/<br>{algorithm_id}                                        | modelarts:aiAlgorithm:update | -          |
| DELETE /v2/<br>{project_id}/<br>algorithms/<br>{algorithm_id}                                     | modelarts:aiAlgorithm:delete | -          |
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}                                  | modelarts:trainJob:get       | -          |
| PUT /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}                                  | modelarts:trainJob:update    | -          |
| DELETE /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}                               | modelarts:trainJob:delete    | -          |
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>tasks/{task_id}/<br>logs/url | modelarts:trainJob:logExport | -          |
| POST /v2/<br>{project_id}/<br>training-job-<br>searches                                           | modelarts:trainJob:list      | -          |
| POST /v1/<br>{project_id}/<br>networks                                                            | modelarts:network:create     | -          |
| GET /v1/<br>{project_id}/<br>networks/<br>{network_name}                                          | modelarts:network:get        | -          |

| API                                                                                                                         | Action                    | Dependency |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------|------------|
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>autosearch-trials                                      | modelarts:trainJob:get    | -          |
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>autosearch-trials/<br>{trial_id}                       | modelarts:trainJob:get    | -          |
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>autosearch-<br>parameter-analysis                      | modelarts:trainJob:get    | -          |
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>autosearch-<br>parameter-analysis/<br>{parameter_name} | modelarts:trainJob:get    | -          |
| GET /v2/<br>{project_id}/<br>workflows                                                                                      | modelarts:workflow:list   | -          |
| POST /v2/<br>{project_id}/<br>workflows                                                                                     | modelarts:workflow:create | -          |
| DELETE /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}                                                                 | modelarts:workflow:delete | -          |
| GET /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}                                                                    | modelarts:workflow:get    | -          |
| PUT /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}                                                                    | modelarts:workflow:update | -          |

| API                                                                             | Action                     | Dependency |
|---------------------------------------------------------------------------------|----------------------------|------------|
| GET /v2/{project_id}/workflows/overview                                         | modelarts:workflow:list    | -          |
| GET /v2/{project_id}/workflows/todolist                                         | modelarts:workflow:list    | -          |
| GET /v2/{project_id}/workflows/{workflow_id}/executions                         | modelarts:workflow:list    | -          |
| POST /v2/{project_id}/workflows/{workflow_id}/executions                        | modelarts:workflow:execute | -          |
| DELETE /v2/{project_id}/workflows/{workflow_id}/executions/{execution_id}       | modelarts:workflow:delete  | -          |
| GET /v2/{project_id}/workflows/{workflow_id}/executions/{execution_id}          | modelarts:workflow:get     | -          |
| PUT /v2/{project_id}/workflows/{workflow_id}/executions/{execution_id}          | modelarts:workflow:update  | -          |
| POST /v2/{project_id}/workflows/{workflow_id}/executions/{execution_id}/actions | modelarts:workflow:execute | -          |

| API                                                                                                                                                 | Action                     | Dependency |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|------------|
| POST /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>executions/<br>{execution_id}/step-<br>executions/<br>{step_execution_id}/<br>actions | modelarts:workflow:execute | -          |
| GET /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>executions/<br>{execution_id}/step-<br>executions/<br>{step_execution_id}/<br>metrics  | modelarts:workflow:get     | -          |
| DELETE /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>subscriptions/<br>{subscription_id}                                                 | modelarts:workflow:delete  | -          |
| GET /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>subscriptions/<br>{subscription_id}                                                    | modelarts:workflow:get     | -          |
| PUT /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>subscriptions/<br>{subscription_id}                                                    | modelarts:workflow:update  | -          |
| GET /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>schedules/<br>{schedule_id}                                                            | modelarts:workflow:get     | -          |

| API                                                                                         | Action                               | Dependency |
|---------------------------------------------------------------------------------------------|--------------------------------------|------------|
| DELETE /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>schedules/<br>{schedule_id} | modelarts:workflow:delete            | -          |
| PUT /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>schedules/<br>{schedule_id}    | modelarts:workflow:update            | -          |
| GET /v1/<br>{project_id}/<br>workspaces/<br>{workspace_id}                                  | modelarts:workspace:get              | -          |
| PUT /v1/<br>{project_id}/<br>workspaces/<br>{workspace_id}                                  | modelarts:workspace:updat<br>e       | -          |
| DELETE /v1/<br>{project_id}/<br>workspaces/<br>{workspace_id}                               | modelarts:workspace:delete           | -          |
| GET /v1/<br>{project_id}/<br>workspaces/<br>{workspace_id}/<br>quotas                       | modelarts:workspace:getQu<br>otas    | -          |
| PUT /v1/<br>{project_id}/<br>workspaces/<br>{workspace_id}/<br>quotas                       | modelarts:workspace:updat<br>eQuotas | -          |
| GET /v2/<br>{project_id}/<br>datasets                                                       | modelarts:dataset:list               | -          |
| POST /v2/<br>{project_id}/<br>datasets                                                      | modelarts:dataset:create             | -          |
| GET /v1/<br>{project_id}/<br>workspaces                                                     | modelarts:workspace:list             | -          |

| API                                                                                  | Action                               | Dependency |
|--------------------------------------------------------------------------------------|--------------------------------------|------------|
| POST /v1/<br>{project_id}/<br>workspaces                                             | modelarts:workspace:create           | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}                               | modelarts:dataset:get                | -          |
| PUT /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}                               | modelarts:dataset:update             | -          |
| DELETE /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}                            | modelarts:dataset:delete             | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/stats    | modelarts:dataset:get                | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/metrics                       | modelarts:dataset:get                | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/<br>versions                  | modelarts:dataset:get                | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/<br>versions                 | modelarts:dataset:publishV<br>ersion | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/<br>versions/<br>{version_id} | modelarts:dataset:get                | -          |

| API                                                                                                     | Action                          | Dependency |
|---------------------------------------------------------------------------------------------------------|---------------------------------|------------|
| DELETE /v2/{project_id}/datasets/{dataset_id}/versions/{version_id}                                     | modelarts:dataset:deleteVersion | -          |
| GET /v2/{project_id}/datasets/{dataset_id}/data-annotations/samples                                     | modelarts:dataAnnotation:list   | -          |
| POST /v2/{project_id}/datasets/{dataset_id}/data-annotations/samples                                    | modelarts:dataAnnotation:upload | -          |
| POST /v2/{project_id}/datasets/{dataset_id}/data-annotations/samples/delete                             | modelarts:dataAnnotation:delete | -          |
| GET /v2/{project_id}/datasets/{dataset_id}/data-annotations/samples/{sample_id}                         | modelarts:dataAnnotation:get    | -          |
| GET /v2/{project_id}/datasets/{dataset_id}/data-annotations/search-condition                            | modelarts:dataAnnotation:list   | -          |
| GET /v2/{project_id}/datasets/{dataset_id}/workforce-tasks/{workforce_task_id}/data-annotations/samples | modelarts:dataAnnotation:list   | -          |

| API                                                                                                                                                 | Action                              | Dependency |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|------------|
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/<br>workforce-tasks/<br>{workforce_task_id}<br>/data-annotations/<br>samples/<br>{sample_id} | modelarts:dataAnnotation:<br>get    | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/labels                                                                  | modelarts:dataAnnotation:li<br>st   | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/labels                                                                 | modelarts:dataAnnotation:c<br>reate | -          |
| PUT /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/labels                                                                  | modelarts:dataAnnotation:<br>update | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/labels/<br>delete                                                      | modelarts:dataAnnotation:<br>delete | -          |
| PUT /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/labels/<br>{label_name}                                                 | modelarts:dataAnnotation:<br>update | -          |
| DELETE /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/labels/<br>{label_name}                                              | modelarts:dataAnnotation:<br>delete | -          |



| API                                                                                     | Action                              | Dependency |
|-----------------------------------------------------------------------------------------|-------------------------------------|------------|
| PUT /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/data-<br>annotations/<br>samples | modelarts:dataAnnotation:<br>update | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/import-<br>tasks                 | modelarts:dataset:get               | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/import-<br>tasks                | modelarts:dataset:import            | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/import-<br>tasks/{task_id}       | modelarts:dataset:get               | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/export-<br>tasks                 | modelarts:dataset:get               | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/export-<br>tasks                | modelarts:dataset:export            | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{resource_id}/<br>export-tasks/<br>{task_id}  | modelarts:dataset:get               | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/sync-<br>data                   | modelarts:dataset:update            | -          |

| API                                                                                                     | Action                            | Dependency |
|---------------------------------------------------------------------------------------------------------|-----------------------------------|------------|
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/sync-<br>data/status                             | modelarts:dataset:get             | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/auto-<br>annotations/<br>samples                 | modelarts:dataAnnotation:li<br>st | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/auto-<br>annotations/<br>samples/<br>{sample_id} | modelarts:dataAnnotation:<br>get  | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/tasks                                            | modelarts:dataset:get             | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/tasks                                           | modelarts:dataset:update          | -          |
| GET /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/tasks/<br>{task_id}                              | modelarts:dataset:get             | -          |
| POST /v2/<br>{project_id}/<br>datasets/<br>{dataset_id}/tasks/<br>{task_id}/stop                        | modelarts:dataset:update          | -          |
| PUT /v1/<br>{project_id}/<br>services/{service_id}                                                      | modelarts:service:update          | -          |
| PUT /v1/<br>{project_id}/<br>services/<br>{service_id}/nodes/<br>{node_id}/status                       | modelarts:nodeservice:actio<br>n  | -          |

| API                                                        | Action                      | Dependency |
|------------------------------------------------------------|-----------------------------|------------|
| GET /v1/{project_id}/services/{service_id}/events          | modelarts:service:getEvents | -          |
| POST /v1/{project_id}/services/{resource_id}/tags/create   | modelarts:service:update    | -          |
| DELETE /v1/{project_id}/services/{resource_id}/tags/delete | modelarts:service:update    | -          |
| GET /v1/{project_id}/services/tms/tags                     | modelarts:service:get       | -          |
| DELETE /v1/{project_id}/services/{service_id}              | modelarts:service:delete    | -          |
| GET /v1/{project_id}/services/{service_id}                 | modelarts:service:get       | -          |
| GET /v1/{project_id}/services/{service_id}/logs            | modelarts:service:getLogs   | -          |
| POST /v1/{project_id}/services                             | modelarts:service:create    | -          |
| GET /v1/{project_id}/networks                              | modelarts:network:list      | -          |
| DELETE /v1/{project_id}/networks/{network_name}            | modelarts:network:delete    | -          |
| PATCH /v1/{project_id}/networks/{network_name}             | modelarts:network:update    | -          |
| GET /v2/{project_id}/pools/{pool_name}/nodes               | modelarts:pool:get          | -          |

| API                                                                         | Action                     | Dependency |
|-----------------------------------------------------------------------------|----------------------------|------------|
| POST /v2/<br>{project_id}/pools/<br>{pool_name}/<br>nodes/batch-delete      | modelarts:pool:update      | -          |
| GET /v1/<br>{project_id}/events                                             | modelarts:pool:get         | -          |
| POST /v2/<br>{project_id}/pools                                             | modelarts:pool:create      | -          |
| GET /v2/<br>{project_id}/pools                                              | modelarts:pool:list        | -          |
| GET /v2/<br>{project_id}/pools/<br>{pool_name}                              | modelarts:pool:get         | -          |
| DELETE /v2/<br>{project_id}/pools/<br>{pool_name}                           | modelarts:pool:delete      | -          |
| PATCH /v2/<br>{project_id}/pools/<br>{pool_name}                            | modelarts:pool:update      | -          |
| GET /v2/<br>{project_id}/pools/<br>{pool_name}/<br>monitor                  | modelarts:pool:get         | -          |
| GET /v2/<br>{project_id}/<br>statistics/pools                               | modelarts:pool:list        | -          |
| GET /v2/<br>{project_id}/pools/<br>{pool_name}/<br>workloads                | modelarts:pool:get         | -          |
| GET /v2/<br>{project_id}/<br>statistics/pools/<br>{pool_name}/<br>workloads | modelarts:pool:get         | -          |
| POST /v1/<br>{project_id}/dev-<br>servers                                   | modelarts:devserver:create | -          |
| GET /v1/<br>{project_id}/dev-<br>servers/{id}                               | modelarts:devserver:get    | -          |

| API                                                                                                   | Action                       | Dependency |
|-------------------------------------------------------------------------------------------------------|------------------------------|------------|
| DELETE /v1/<br>{project_id}/dev-<br>servers/{id}                                                      | modelarts:devserver:delete   | -          |
| PUT /v1/<br>{project_id}/dev-<br>servers/sync                                                         | modelarts:devserver:sync     | -          |
| PUT /v1/<br>{project_id}/dev-<br>servers/{id}/start                                                   | modelarts:devserver:start    | -          |
| PUT /v1/<br>{project_id}/dev-<br>servers/{id}/stop                                                    | modelarts:devserver:stop     | -          |
| GET /v1/<br>{project_id}/images/<br>group                                                             | modelarts:image:listGroup    | -          |
| POST /v2/<br>{project_id}/<br>training-jobs                                                           | modelarts:trainJob:logExport | -          |
| POST /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>actions                         | modelarts:trainJob:create    | -          |
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>tasks/{task_id}/logs/<br>preview | modelarts:trainJob:get       | -          |
| GET /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>metrics/{task_id}                | modelarts:trainJob:get       | -          |
| POST /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>subscriptions                           | modelarts:workflow:update    | -          |

| API                                                                                                             | Action                    | Dependency |
|-----------------------------------------------------------------------------------------------------------------|---------------------------|------------|
| POST /v2/<br>{project_id}/<br>workflows/<br>{workflow_id}/<br>schedules                                         | modelarts:workflow:update | -          |
| GET /v2/<br>{project_id}/metrics/<br>runtime/pools                                                              | modelarts:pool:list       | -          |
| POST /v2/<br>{project_id}/<br>training-jobs/<br>{training_job_id}/<br>autosearch-trial-<br>earlystop/{trial_id} | modelarts:trainJob:get    | -          |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-180](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for modelarts.

**Table 3-180** Resource types supported by modelarts

| Resource Type  | URN                                                                 |
|----------------|---------------------------------------------------------------------|
| workspace      | modelarts:<region>:<account-id>:workspace:<workspace-id>            |
| dataAnnotation | modelarts:<region>:<account-id>:dataAnnotation:<data-annotation-id> |
| trainJob       | modelarts:<region>:<account-id>:trainJob:<train-job-id>             |
| devserver      | modelarts:<region>:<account-id>:devserver:<devserver-id>            |
| image          | modelarts:<region>:<account-id>:image:<image-id>                    |
| service        | modelarts:<region>:<account-id>:service:<service-id>                |
| network        | modelarts:<region>:<account-id>:network:<network-id>                |
| pool           | modelarts:<region>:<account-id>:pool:<pool-id>                      |

| Resource Type | URN                                                           |
|---------------|---------------------------------------------------------------|
| model         | modelarts:<region>:<account-id>:model:<model-id>              |
| workflow      | modelarts:<region>:<account-id>:workflow:<workflow-id>        |
| aiAlgorithm   | modelarts:<region>:<account-id>:aiAlgorithm:<ai-algorithm-id> |
| dataset       | modelarts:<region>:<account-id>:dataset:<dataset-id>          |
| nodeservice   | modelarts:<region>:<account-id>:nodeservice:<node-service-id> |
| notebook      | modelarts:<region>:<account-id>:notebook:<notebook-id>        |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, modelarts) apply only to operations of the xx service. For details, see [Table 3-181](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by modelarts

The following table lists the condition keys that you can define in identity policies for modelarts. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-181** Service-specific condition keys supported by modelarts

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                         |
|--------------------------------|--------|-------------------------------|-------------------------------------|
| modelarts:poolType             | string | Single-valued                 | Filters access ModelArts pool type. |
| modelarts:poolId               | string | Single-valued                 | Filters access ModelArts pool ID.   |

## 3.9 Analytics

### 3.9.1 Cloud Search Service (CSS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Action

Actions are specific operations that are allowed in an identity policy.

- The **Access Level** column describes how the action is classified (such as **list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.



- You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
- If this column includes a resource type, you must specify the URN in the Resource element of your statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CSS, see [Resource Type](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about condition keys defined by CSS, see [Condition](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CSS.

**Table 3-182** Actions supported by CSS

| Action                          | Description                                                            | Access Level | Resource Type (*: Required) | Condition Key                                                                                                      | Alias |
|---------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------|-------|
| css:VPCEndpoint:updateWhitelist | Grant the permission to update an existing whitelist of VPC endpoints. | write        | cluster *                   | <ul style="list-style-type: none"> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:log:updateBackupPolicy      | Grant the permission to modify or delete log backups.                  | write        | cluster *                   | <ul style="list-style-type: none"> <li>• g:EnterpriseProjectId</li> <li>• g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                               | Description                                                   | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|--------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:snapshot:setSnapshotPolicy       | Grant the permission to set backup policies.                  | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:snapshot:getSnapshotPolicy       | Grant the permission to query backup policies.                | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:snapshot:restore                 | Grant the permission to restore data from a snapshot.         | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:snapshot:create                  | Grant the permission to create a snapshot.                    | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:publicIpAddress:associates       | Grant the permission to enable or disable public access.      | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:publicIpAddress:setAccessControl | Grant the permission to manage whitelists for access control. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:tag:get                          | Grant the permission to query resource tags.                  | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                                | Description                                                | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias                  |
|---------------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|------------------------|
| css:publicIpAddress:modifyBandwidth   | Grant the permission to modify the bandwidth size.         | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                      |
| css:VPCEndpoint:enableOrDisable       | Grant the permission to create or delete a VPCEP.          | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                      |
| css:log:getBasicConfigurations        | Grant the permission to query basic configurations.        | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                      |
| css:snapshot:list                     | Grant the permission to view the snapshot list.            | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                      |
| css:log:list                          | Grant the permission to view logs.                         | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                      |
| css:snapshot:setSnapshotConfiguration | Grant the permission to set basic snapshot configurations. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                      |
| css:cluster:listFlavors               | Grant the permission to query the flavor ID list.          | list         | -                           | -                                                                                                              | css:cluster:showFlavor |
| css:cluster:listDiskType              | Grant the permission to list available disk types.         | list         | -                           | -                                                                                                              | -                      |

| Action                               | Description                                                                     | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias                   |
|--------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------|
| css:tag:list                         | Grant the permission to query project tags.                                     | list         | cluster *                   | -                                                                                                              | -                       |
| css:VPCEndpoint:manageConnection     | Grant the permission to configure the connection of the endpoint.               | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                       |
| css:log:listJob                      | Grant the permission to query the job list.                                     | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                       |
| css:cluster:downloadCert             | Grant the permission to obtain the content of a certificate.                    | read         | -                           | -                                                                                                              | -                       |
| css:cluster:get                      | Grant the permission to query cluster details.                                  | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | css:cluster:getInstance |
| css:snapshot:enableAutomaticSnapshot | Grant the permission to set basic configurations for automatic snapshot backup. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                       |
| css:snapshot:delete                  | Grant the permission to delete a specified snapshot.                            | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                       |

| Action                           | Description                                                            | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias                    |
|----------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|--------------------------|
| css:IKThesaurus:get              | Grant the permission to view the custom word dictionary configuration. | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                        |
| css:cluster:restart              | Grant the permission to restart an Elasticsearch cluster.              | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                        |
| css:cluster:modifySecurityGroup  | Grant the permission to modify the cluster security group.             | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                        |
| css:configurations:list          | Grant the permission to query parameter settings.                      | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                        |
| css:cluster:delete               | Grant the permission to delete a cluster.                              | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                        |
| css:cluster:modifySpecifications | Grant the permission to modify cluster specifications.                 | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                        |
| css:cluster:list                 | Grant the permission to list cluster information.                      | list         | cluster *                   | -                                                                                                              | css:cluster:getInstances |

| Action                               | Description                                                                       | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|--------------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:cluster:scaleOut                 | Grant the permission to scale out a cluster.                                      | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:IKThesaurus:load                 | Grant the permission to load a custom word dictionary.                            | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:configurations:modify            | Grant permission to update parameter settings.                                    | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:configurations:get               | Grant the permission to obtain the parameter list.                                | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:IKThesaurus:delete               | Grant the permission to delete a word dictionary.                                 | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:expand                   | Grant the permission to scale out the quantity and storage capacity of instances. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:snapshot:disableSnapshotFunction | Grant the permission to disable the cluster snapshot function.                    | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                          | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|---------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:cluster:upgradeCluster      | Grant the permission to upgrade clusters or replace nodes.      | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:VPCEndpoint:listConnections | Grant the permission to query VPCEP connections.                | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:scaleIn             | Grant the permission to scale in a cluster.                     | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:log:setBasicConfigurations  | Grant the permission to set basic configurations.               | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:tag:addOrDelete             | Grant the permission to add or delete resource tags in batches. | tagging      | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
|                                 |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>              |       |
| css:publicKibana:close          | Grant the permission to disable public access.                  | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                 | Description                                                                     | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                    | Alias |
|------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------|
| css:tag:edit           | Grant the permission to modify cluster tags.                                    | tagging      | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>                   | -     |
|                        |                                                                                 |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                                |       |
| css:cluster:create     | Grant the permission to create a cluster.                                       | write        | cluster *                   | -                                                                                                                                | -     |
|                        |                                                                                 |              | -                           | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |       |
| css:cluster:topPeriod  | Grant the permission to change the billing mode of a cluster to yearly/monthly. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>                   | -     |
| css:cluster:modifyName | Grant the permission to change the cluster name.                                | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>                   | -     |
| css:log:backup         | Grant the permission to back up logs.                                           | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul>                   | -     |



| Action                            | Description                                          | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias                              |
|-----------------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|------------------------------------|
| css:cluster:closeLogSetting       | Grant the permission to disable logging.             | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | css:log:enableOrDisableLogFunction |
| css:cluster:openLogSetting        | Grant the permission to enable logging.              | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | css:log:enableOrDisableLogFunction |
| css:cluster:modifyPassword        | Grant the permission to change the cluster password. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                  |
| css:publicIpAddress:disassociates | Grant the permission to unbind public networks.      | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                  |
| css:publicIpAddress:open          | Grant the permission to bind public networks.        | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                  |
| css:tag:delete                    | Grant the permission to delete a tag.                | tagging      | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                  |
|                                   |                                                      |              | -                           | g:TagKeys                                                                                                      |                                    |
| css:cluster:shrinkNodes           | Grant the permission to scale in a specified node.   | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                                  |

| Action                           | Description                                                                    | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias                      |
|----------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------|
| css:cluster:changeMode           | Grant the permission to modify the security mode.                              | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                          |
| css:cluster:addIndependenceNodes | Grant the permission to add independent master and client nodes.               | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                          |
| css:cluster:rollingReboot        | Grant the permission to perform a rolling restart of an Elasticsearch cluster. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | css:cluster:rollingRestart |
| css:logstash:listActions         | Grant the permission to query operation records.                               | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                          |
| css:cluster:uploadCerts          | Grant the permission to upload certificates.                                   | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                          |
| css:cluster:deleteCerts          | Grant the permission to delete certificates.                                   | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                          |
| css:cluster:listCerts            | Grant the permission to query the certificate list.                            | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | css:cluster:getCertsList   |

| Action                          | Description                                                                   | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias                           |
|---------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------|
| css:cluster:getCertsDetail      | Grant the permission to query certificate details.                            | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                               |
| css:logstash:deleteConfTemplate | Grant the permission to delete a custom template.                             | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                               |
| css:logstash:listConfigTemplate | Grant the permission to query the template list.                              | list         | -                           | -                                                                                                              | css:logstash:configListTemplate |
| css:logstash:confStop           | Grant the permission to stop or hot-stop pipeline tasks for data migration.   | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                               |
| css:logstash:checkConnection    | Grant the permission to test the connectivity.                                | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                               |
| css:logstash:confDelete         | Grant the permission to delete configuration files.                           | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                               |
| css:logstash:confStart          | Grant the permission to start or hot-start pipeline tasks for data migration. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -                               |

| Action                       | Description                                                             | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:logstash:getConfDetail   | Grant the permission to query the content of configuration files.       | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:azmigrate        | Grant the permission to switch AZs.                                     | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:logstash:confUpdate      | Grant the permission to update configuration files.                     | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:logstash:listPipelines   | Grant the permission to query the pipeline list.                        | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:retryAction      | Grant the permission to retry a task or terminate the impact of a task. | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:logstash:listConfs       | Grant the permission to query the configuration file list.              | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:logstash:configFavorites | Grant the permission to add items to a custom template.                 | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                         | Description                                                              | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|--------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:cluster:listUpgradeCluster | Grant the permission to obtain the upgrade image ID and upgrade details. | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:logstash:submitConf        | Grant the permission to create configuration files.                      | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:plugin:list                | Grant the permission to query the cluster plug-in list.                  | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:plugin:getOperationRecords | Grant the permission to query the plug-in operation records.             | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:plugin:delete              | Grant the permission to delete plug-ins.                                 | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:plugin:installOrUninstall  | Grant the permission to install or uninstall plug-ins.                   | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:plugin:upload              | Grant the permission to upload plug-ins.                                 | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                               | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|--------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:plugin:getDefault                | Grant the permission to query default plug-ins.                 | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:getAgencies              | Grant the permission to obtain agents.                          | read         | -                           | -                                                                                                              | -     |
| css:cluster:modifyRoute              | Grant the permission to modify cluster routes.                  | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:getRoutes                | Grant the permission to obtain the cluster routes.              | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:logstash:actionList              | Grant the permission to query the cluster task list.            | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:createUserInfo           | Grant the permission to query information about a created user. | write        | cluster *                   | -                                                                                                              | -     |
| css:VPCEndpoint:modifyConnections    | Grant the permission to modify the size of a connection.        | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:queryNeedDeleteInstances | Grant the permission to query the node to be deleted.           | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                           | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| css:cluster:queryKey             | Grant the permission to obtain keys.                                | read         | -                           | -             | -     |
| css:cluster:queryKeys            | Grant the permission to obtain the key list.                        | list         | -                           | -             | -     |
| css:cluster:getPubliczonePicture | Grant the permission to obtain the bandwidth price.                 | read         | cluster *                   | -             | -     |
| css:datastore:get                | Grant the permission to obtain the data engine.                     | read         | cluster *                   | -             | -     |
| css:datastore:list               | Grant the permission to obtain the data engine list.                | list         | cluster *                   | -             | -     |
| css:cluster:getDiskUsage         | Grant the permission to obtain the cluster storage capacity status. | read         | cluster *                   | -             | -     |
| css:snapshot:showDetail          | Grant the permission to obtain snapshot details.                    | read         | cluster *                   | -             | -     |
| css:cluster:getAvailableBuckets  | Grant the permission to obtain an available OBS bucket.             | list         | -                           | -             | -     |

| Action                              | Description                                             | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|-------------------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:cluster:checkCssName            | Grant the permission to check cluster names.            | write        | cluster *                   | -                                                                                                              | -     |
| css:snapshot:deleteAllFailedTask    | Grant the permission to delete all failed tasks.        | write        | -                           | -                                                                                                              | -     |
| css:snapshot:deleteSingleFailedTask | Grant the permission to delete specified failed tasks.  | write        | -                           | -                                                                                                              | -     |
| css:snapshot:getAllFailedTask       | Grant the permission to view failed backup tasks.       | list         | -                           | -                                                                                                              | -     |
| css::createServiceAgency            | Grant the permission to create agencies.                | write        | -                           | -                                                                                                              | -     |
| css:cluster:createAiOps             | Grant the permission to create detection tasks.         | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:listAiOps               | Grant the permission to obtain the detection task list. | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:deleteAiOps             | Grant the permission to delete detection tasks.         | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |



| Action                        | Description                                                                                  | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|-------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:cluster:listSmnTopics     | Grant the permission to obtain the SMN topic list.                                           | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:listElbs          | Grant the permission to obtain the list of available load balancers for the current cluster. | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:elbSwitch         | Grant the permission to enable or disable load balancing.                                    | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:createElbListener | Grant the permission to create listeners for the current cluster.                            | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:updateElbListener | Grant the permission to modify listeners for the current cluster.                            | write        | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |
| css:cluster:getElbDetail      | Grant the permission to query information about load balancers used by the current cluster.  | read         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

| Action                   | Description                                                        | Access Level | Resource Type (*: Required) | Condition Key                                                                                                  | Alias |
|--------------------------|--------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-------|
| css:cluster:listElbCerts | Grant the permission to obtain the load balancer certificate list. | list         | cluster *                   | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> | -     |

Each API of CSS usually supports one or more actions. [Table 3-183](#) lists the supported actions and dependencies.

**Table 3-183** Actions and dependencies supported by CSS APIs

| API                              | Action             | Dependency                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters | css:cluster:create | <ul style="list-style-type: none"> <li>ecs:cloudServerFlavors:get</li> <li>evs:types:get</li> <li>vpc:vpcs:list</li> <li>vpc:securityGroups:list</li> <li>vpc:securityGroups:get</li> <li>vpc:subnets:list</li> <li>vpc:subnets:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>vpc:ports:delete</li> <li>vpc:ports:get</li> <li>css:cluster:getAgencies</li> <li>iam:agencies:listAgencies</li> <li>iam:permissions:listRolesForAgency</li> <li>iam:permissions:listRolesForAgencyOnProject</li> <li>iam:agencies:pass</li> </ul> |

| API                                                       | Action                          | Dependency                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2.0/{project_id}/clusters                          | css:cluster:create              | <ul style="list-style-type: none"> <li>• ecs:cloudServerFlavors:get</li> <li>• evs:types:get</li> <li>• vpc:vpcs:list</li> <li>• vpc:securityGroups:list</li> <li>• vpc:securityGroups:get</li> <li>• vpc:subnets:list</li> <li>• vpc:subnets:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> <li>• vpc:ports:delete</li> <li>• vpc:ports:get</li> <li>• css:cluster:getAgencies</li> <li>• iam:agencies:listAgencies</li> <li>• iam:permissions:listRolesForAgency</li> <li>• iam:permissions:listRolesForAgencyOnProject</li> <li>• iam:agencies:pass</li> </ul> |
| POST /v1.0/{project_id}/clusters/{cluster_id}/sg/change   | css:cluster:modifySecurityGroup | <ul style="list-style-type: none"> <li>• vpc:securityGroups:list</li> <li>• vpc:ports:update</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| GET /v1.0/{project_id}/clusters                           | css:cluster:list                | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| GET /v1.0/{project_id}/clusters/{cluster_id}              | css:cluster:get                 | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}           | css:cluster:delete              | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| POST /v1.0/{project_id}/cluster/{cluster_id}/period       | css:cluster:toPeriod            | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| POST /v1.0/{project_id}/clusters/{cluster_id}/changenname | css:cluster:modifyName          | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| API                                                          | Action                           | Dependency                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters/{cluster_id}/password/reset | css:cluster:modifyPassword       | -                                                                                                                                                                                                                                                                                                    |
| POST /v1.0/{project_id}/clusters/{cluster_id}/restart        | css:cluster:restart              | -                                                                                                                                                                                                                                                                                                    |
| POST /v2.0/{project_id}/clusters/{cluster_id}/restart        | css:cluster:restart              | -                                                                                                                                                                                                                                                                                                    |
| POST /v1.0/{project_id}/clusters/{cluster_id}/extend         | css:cluster:scaleOut             | <ul style="list-style-type: none"> <li>• ecs:cloudServerFlavors:get</li> <li>• evs:types:get</li> <li>• vpc:vpcs:list</li> <li>• vpc:subnets:list</li> <li>• vpc:subnets:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> <li>• vpc:ports:delete</li> <li>• vpc:ports:get</li> </ul> |
| POST /v1.0/{project_id}/clusters/{cluster_id}/role_extend    | css:cluster:expand               | <ul style="list-style-type: none"> <li>• ecs:cloudServerFlavors:get</li> <li>• evs:types:get</li> <li>• vpc:vpcs:list</li> <li>• vpc:subnets:list</li> <li>• vpc:subnets:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> <li>• vpc:ports:delete</li> <li>• vpc:ports:get</li> </ul> |
| POST /v1.0/{project_id}/clusters/{cluster_id}/flavor         | css:cluster:modifySpecifications | ecs:cloudServerFlavors:get                                                                                                                                                                                                                                                                           |
| GET /v1.0/{project_id}/es-flavors                            | css:cluster:listFlavors          | ecs:cloudServerFlavors:get                                                                                                                                                                                                                                                                           |

| API                                                                         | Action                           | Dependency                                                                                                                                                                   |
|-----------------------------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1.0/{project_id}/{resource_type}/tags                                 | css:tag:list                     | -                                                                                                                                                                            |
| GET /v1.0/{project_id}/{resource_type}/{cluster_id}/tags                    | css:tag:get                      | -                                                                                                                                                                            |
| POST /v1.0/{project_id}/{resource_type}/{cluster_id}/tags                   | css:tag:edit                     | -                                                                                                                                                                            |
| DELETE /v1.0/{project_id}/{resource_type}/{cluster_id}/tags/{key}           | css:tag:delete                   | -                                                                                                                                                                            |
| POST /v1.0/{project_id}/{resource_type}/{cluster_id}/tags/action            | css:tag:addOrDelete              | -                                                                                                                                                                            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/{types}/flavor                | css:cluster:modifySpecifications | ecs:cloudServerFlavors:get                                                                                                                                                   |
| POST /v1.0/extend/{project_id}/clusters/{cluster_id}/role/shrink            | css:cluster:scaleIn              | <ul style="list-style-type: none"> <li>iam:agencies:listAgencies</li> <li>iam:permissions:listRolesForAgency</li> <li>iam:permissions:listRolesForAgencyOnProject</li> </ul> |
| GET /v1.0/{project_id}/cer/download                                         | css:cluster:downloadCert         | -                                                                                                                                                                            |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/instance/{instance_id}/replace | css:cluster:upgradeCluster       | <ul style="list-style-type: none"> <li>iam:agencies:listAgencies</li> <li>iam:permissions:listRolesForAgency</li> <li>iam:permissions:listRolesForAgencyOnProject</li> </ul> |

| API                                                                               | Action                           | Dependency                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters/{cluster_id}/node/offline                        | css:cluster:shrinkNodes          | <ul style="list-style-type: none"> <li>iam:agencies:listAgencies</li> <li>iam:permissions:listRolesForAgency</li> <li>iam:permissions:listRolesForAgencyOnProject</li> </ul>                                                                                                       |
| POST /v1.0/{project_id}/clusters/{cluster_id}/mode/change                         | css:cluster:changeMode           | -                                                                                                                                                                                                                                                                                  |
| POST /v1.0/{project_id}/clusters/{cluster_id}/type/{type}/independent             | css:cluster:addIndependenceNodes | <ul style="list-style-type: none"> <li>ecs:cloudServerFlavors:get</li> <li>evs:types:get</li> <li>vpc:vpcs:list</li> <li>vpc:subnets:list</li> <li>vpc:subnets:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>vpc:ports:delete</li> <li>vpc:ports:get</li> </ul> |
| POST /v1.0/{project_id}/clusters/{cluster_id}/inst-type/{inst_type}/image/upgrade | css:cluster:upgradeCluster       | -                                                                                                                                                                                                                                                                                  |
| POST /v1.0/{project_id}/clusters/{cluster_id}/inst-type/{inst_type}/azmigrate     | css:cluster:azmigrate            | <ul style="list-style-type: none"> <li>iam:agencies:listAgencies</li> <li>iam:permissions:listRolesForAgency</li> <li>iam:permissions:listRolesForAgencyOnProject</li> </ul>                                                                                                       |
| GET /v1.0/{project_id}/clusters/{cluster_id}/upgrade/detail                       | css:cluster:listUpgradeCluster   | -                                                                                                                                                                                                                                                                                  |

| API                                                                       | Action                              | Dependency                                                                                                                                                                                           |
|---------------------------------------------------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1.0/{project_id}/clusters/{cluster_id}/target/{upgrade_type}/images | css:cluster:listUpgradeCluster      | -                                                                                                                                                                                                    |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/upgrade/{action_id}/retry    | css:cluster:retryAction             | -                                                                                                                                                                                                    |
| POST /v1.0/{project_id}/clusters/{cluster_id}/thesaurus                   | css:IKThesaurus:load                | <ul style="list-style-type: none"> <li>• obs:bucket:listAllMyBuckets</li> <li>• obs:bucket:getBucketLocation</li> <li>• obs:bucket:getBucketStoragePolicy</li> <li>• obs:object:getObject</li> </ul> |
| GET /v1.0/{project_id}/clusters/{cluster_id}/thesaurus                    | css:IKThesaurus:get                 | -                                                                                                                                                                                                    |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}/thesaurus                 | css:IKThesaurus:delete              | -                                                                                                                                                                                                    |
| POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/open           | css:publicKibana:open               | -                                                                                                                                                                                                    |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/publickibana/close           | css:publicKibana:close              | -                                                                                                                                                                                                    |
| POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/bandwidth      | css:publicIPAddress:modifyBandwidth | -                                                                                                                                                                                                    |

| API                                                                         | Action                               | Dependency                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters/{cluster_id}/publickibana/whitelist/update | css:publicIPAddress:setAccessControl | -                                                                                                                                                                                                                                      |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/publickibana/whitelist/close   | css:publicIPAddress:setAccessControl | -                                                                                                                                                                                                                                      |
| POST /v1.0/{project_id}/clusters/{cluster_id}/logs/open                     | css:cluster:openLogSetting           | <ul style="list-style-type: none"> <li>• iam:agencies:pass</li> <li>• obs:bucket:listAllMyBuckets</li> <li>• obs:bucket:getBucketLocation</li> <li>• obs:bucket:getBucketStoragePolicy</li> <li>• iam:agencies:listAgencies</li> </ul> |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/logs/close                     | css:cluster:closeLogSetting          | -                                                                                                                                                                                                                                      |
| GET /v1.0/{project_id}/clusters/{cluster_id}/logs/records                   | css:log:listJob                      | -                                                                                                                                                                                                                                      |
| GET /v1.0/{project_id}/clusters/{cluster_id}/logs/settings                  | css:log:getBasicConfigurations       | -                                                                                                                                                                                                                                      |



| API                                                              | Action                              | Dependency                                                                                                                                                                                                                   |
|------------------------------------------------------------------|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters/{cluster_id}/logs/settings      | css:log:setBasicConfigurations      | <ul style="list-style-type: none"> <li>obs:bucket:listAllMyBuckets</li> <li>obs:bucket:getBucketLocation</li> <li>obs:bucket:getBucketStoragePolicy</li> <li>iam:agencies:listAgencies</li> <li>iam:agencies:pass</li> </ul> |
| POST /v1.0/{project_id}/clusters/{cluster_id}/logs/policy/update | css:log:updateBackupPolicy          | -                                                                                                                                                                                                                            |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/logs/policy/close   | css:log:updateBackupPolicy          | -                                                                                                                                                                                                                            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/logs/collect       | css:log:backup                      | -                                                                                                                                                                                                                            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/logs/search        | css:log:list                        | -                                                                                                                                                                                                                            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/public/open        | css:publicIPAddress:associates      | -                                                                                                                                                                                                                            |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/public/close        | css:publicIPAddress:disassociates   | -                                                                                                                                                                                                                            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/public/bandwidth   | css:publicIPAddress:modifyBandwidth | -                                                                                                                                                                                                                            |

| API                                                                                | Action                                | Dependency                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters/{cluster_id}/public/whitelist/update              | css:publicIPAddress:setAccessControl  | -                                                                                                                                                                                                                                      |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/public/whitelist/close                | css:publicIPAddress:setAccessControl  | -                                                                                                                                                                                                                                      |
| POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/auto_setting          | css:snapshot:enableAutomaticSnapshot  | <ul style="list-style-type: none"> <li>• obs:bucket:createBucket</li> <li>• obs:bucket:headBucket</li> <li>• iam:agencies:listAgencies</li> <li>• iam:agencies:createAgency</li> <li>• iam:permissions:grantRoleToAgency</li> </ul>    |
| POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/setting               | css:snapshot:setSnapshotConfiguration | <ul style="list-style-type: none"> <li>• obs:bucket:listAllMyBuckets</li> <li>• obs:bucket:getBucketLocation</li> <li>• obs:bucket:getBucketStoragePolicy</li> <li>• iam:agencies:listAgencies</li> <li>• iam:agencies:pass</li> </ul> |
| POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot                       | css:snapshot:create                   | iam:agencies:pass                                                                                                                                                                                                                      |
| POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/{snapshot_id}/restore | css:snapshot:restore                  | -                                                                                                                                                                                                                                      |

| API                                                                          | Action                               | Dependency                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/{snapshot_id} | css:snapshot:delete                  | -                                                                                                                                                                                                                                          |
| POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/policy          | css:snapshot:setSnapshotPolicy       | -                                                                                                                                                                                                                                          |
| GET /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/policy           | css:snapshot:getSnapshotPolicy       | -                                                                                                                                                                                                                                          |
| GET /v1.0/{project_id}/clusters/{cluster_id}/index_snapshots                 | css:snapshot:list                    | -                                                                                                                                                                                                                                          |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}/index_snapshots              | css:snapshot:disableSnapshotFunction | -                                                                                                                                                                                                                                          |
| POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/open              | css:VPCEndpoint:enableOrDisable      | <ul style="list-style-type: none"> <li>• vpcep:endpoints:create</li> <li>• vpcep:endpoints:list</li> <li>• vpcep:endpoints:get</li> <li>• vpcep:endpoints:delete</li> <li>• vpcep:endpoints:update</li> </ul>                              |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/close              | css:VPCEndpoint:enableOrDisable      | <ul style="list-style-type: none"> <li>• vpcep::listQuotas</li> <li>• vpcep:endpoints:create</li> <li>• vpcep:endpoints:list</li> <li>• vpcep:endpoints:get</li> <li>• vpcep:endpoints:delete</li> <li>• vpcep:endpoints:update</li> </ul> |

| API                                                                    | Action                           | Dependency          |
|------------------------------------------------------------------------|----------------------------------|---------------------|
| GET /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/connections  | css:VPCEndpoint:listConnection   | vpcep:endpoints:get |
| POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/connections | css:VPCEndpoint:manageConnection | -                   |
| POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/permissions | css:VPCEndpoint:updateWhitelist  | -                   |
| POST /v1.0/{project_id}/clusters/{cluster_id}/ymls/update              | css:configurations:modify        | -                   |
| GET /v1.0/{project_id}/clusters/{cluster_id}/ymls/joblists             | css:configurations:list          | -                   |
| GET /v1.0/{project_id}/clusters/{cluster_id}/ymls/template             | css:configurations:get           | -                   |
| POST /v2.0/{project_id}/clusters/{cluster_id}/snapshots/policy/open    | css:snapshot:setSnapshotPolicy   | -                   |
| PUT /v2.0/{project_id}/clusters/{cluster_id}/snapshots/policy/close    | css:snapshot:setSnapshotPolicy   | -                   |

| API                                                              | Action                          | Dependency |
|------------------------------------------------------------------|---------------------------------|------------|
| POST /v2.0/{project_id}/clusters/{cluster_id}/rolling_restart    | css:cluster:rollingReboot       | -          |
| GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listactions | css:logstash:listActions        | -          |
| DELETE /v1.0/{project_id}/lgsconf/deletetemplate                 | css:logstash:deleteConfTemplate | -          |
| POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/stop       | css:logstash:confStop           | -          |
| POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/hot-stop   | css:logstash:confStop           | -          |
| POST /v1.0/{project_id}/clusters/{cluster_id}/checkconnection    | css:logstash:checkConnection    | -          |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/delete   | css:logstash:confDelete         | -          |
| POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/start      | css:logstash:confStart          | -          |
| POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/hot-start  | css:logstash:confStart          | -          |

| API                                                                                    | Action                              | Dependency |
|----------------------------------------------------------------------------------------|-------------------------------------|------------|
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/lgsconf/<br>confdetail        | css:logstash:getConfDetail          | -          |
| POST /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/lgsconf/<br>update           | css:logstash:confUpdate             | -          |
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/lgsconf/<br>listpipelines     | css:logstash:listPipelines          | -          |
| POST /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/lgsconf/<br>submit           | css:logstash:submitConf             | -          |
| POST /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/lgsconf/<br>favorite         | css:logstash:configFavorites        | -          |
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/lgsconf/<br>listconfs         | css:logstash:listConfs              | -          |
| GET /v1.0/<br>{project_id}/lgsconf/<br>template                                        | css:logstash:listConfigTempl<br>ate | -          |
| POST /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/certs/<br>upload             | css:cluster:uploadCerts             | -          |
| DELETE /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/certs/<br>{cert_id}/delete | css:cluster:deleteCerts             | -          |

| API                                                                               | Action                     | Dependency                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/certs                    | css:cluster:listCerts      | -                                                                                                                                                                                                                       |
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/certs/<br>{cert_id}      | css:cluster:getCertsDetail | -                                                                                                                                                                                                                       |
| POST /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/route                   | css:cluster:modifyRoute    | -                                                                                                                                                                                                                       |
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/route                    | css:cluster:getRoutes      | -                                                                                                                                                                                                                       |
| POST /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/ai-ops                  | css:cluster:createAiOps    | -                                                                                                                                                                                                                       |
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/ai-ops                   | css:cluster:listAiOps      | -                                                                                                                                                                                                                       |
| DELETE /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/ai-ops/<br>{aiops_id} | css:cluster:deleteAiOps    | -                                                                                                                                                                                                                       |
| GET /v1.0/<br>{project_id}/<br>domains/<br>{domain_id}/ai-ops/<br>smn-topics      | css:cluster:listSmnTopics  | <ul style="list-style-type: none"> <li>• css:cluster:getAgencies</li> <li>• iam:agencies:list</li> <li>• iam:agencies:listAgencies</li> <li>• iam:agencies:listAttachedPolicies</li> <li>• iam:agencies:pass</li> </ul> |
| GET /v1.0/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>loadbalancers        | css:cluster:listElbs       | elb:loadbalancers:list                                                                                                                                                                                                  |

| API                                                                     | Action                        | Dependency                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters/{cluster_id}/loadbalancers/es-switch   | css:cluster:elbSwitch         | <ul style="list-style-type: none"> <li>• elb:loadbalancers:list</li> <li>• iam:agencies:listAgencies</li> <li>• iam:permissions:listRolesForAgency</li> <li>• iam:permissions:listRolesForAgencyOnProject</li> <li>• iam:agencies:pass</li> </ul> |
| POST /v1.0/{project_id}/clusters/{cluster_id}/es-listeners              | css:cluster:createElbListener | -                                                                                                                                                                                                                                                 |
| GET /v1.0/{project_id}/clusters/{cluster_id}/es-listeners               | css:cluster:getElbDetail      | -                                                                                                                                                                                                                                                 |
| GET /v1.0/{project_id}/clusters/{cluster_id}/elb/certificates           | css:cluster:listElbCerts      | -                                                                                                                                                                                                                                                 |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/es-listeners/{listener_id} | css:cluster:updateElbListener | -                                                                                                                                                                                                                                                 |

## Resource Type

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-184](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for CSS.



**Table 3-184** Resource types supported by CSS

| Resource Type | URN                                            |
|---------------|------------------------------------------------|
| cluster       | css:<region>:<account-id>:cluster:<cluster-id> |

## Condition

### About condition keys

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **css:**) apply only to operations of the service. For details, see [Table 3-185](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, a condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by CSS

The following table lists the condition keys that you can define in identity policies for CSS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-185** Service-specific condition keys supported by CSS

| Service-specific Condition Key        | Type    | Single-valued/<br>Multivalued | Description                                       |
|---------------------------------------|---------|-------------------------------|---------------------------------------------------|
| <a href="#">css:AssociatePublicIp</a> | boolean | Single-valued                 | Whether to enable public access for the instance. |

### Examples of condition keys

- `css:AssociatePublicIp`

Example: Disallow the creation of CSS clusters that have an EIP associated with it.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "css:cluster:create"
      ],
      "Condition": {
        "Bool": {
          "css:AssociatePublicIp": [
            "true"
          ]
        }
      }
    }
  ]
}
```

Example: Disallow the association of an EIP with a CSS cluster.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "css:publicIpAddress:associates",
        "css:publicKibana:open"
      ]
    }
  ]
}
```

## 3.9.2 Actions Supported by Identity Policy-based Authorization

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied by an SCP in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN for the Resource element in your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DataArts Studio, see [Resources](#).

- **Condition Key** contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DataArts Studio, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in custom identity policies for DataArts Studio.

 NOTE

Due to API restrictions, if the resource type is specified for a custom identity policy, the permission configuration may not meet expectations because some operations are unavailable for specified workspace or instance resources. For example, if an operation that does not support specified resources is allowed but a specific resource is specified for the operation, all resource operations are denied. If an operation that does not support specified resources is denied but a specific resource is specified for the operation, all resource operations are allowed.

Therefore, if you want to specify the resource type for a custom identity policy, you must exclude such operations. Instead, you can only configure identity policies without specified resources or with global resources for such operations, and use multiple identity policies to grant permissions to users. Identity policies without specified resources or with global resources do not contain the **Resource** element in the JSON content, or contain the following **Resource** element:

```
"Resource": [
  "DataArtsStudio:*:*:workspace:*",
  "DataArtsStudio:*:*:instance:*"
]
```

The operations that cannot be performed on specified resources in DataArts Studio are as follows:

- Operations that can be performed only on specified instance resources but not on specified workspace resources:
  - DataArtsStudio:workspace:create
  - DataArtsStudio:workspace:list
- Operations that cannot be performed on specified instance or workspace resources:
  - DataArtsStudio:instance:create
  - DataArtsStudio:instance:get
  - DataArtsStudio:instance:list
  - DataArtsStudio:instance:resize
  - DataArtsStudio:instance:getAgency
  - DataArtsStudio:instance:createAgency
  - DataArtsStudio:instance:uploadDriver
  - DataArtsStudio:instance:deleteDriver
  - DataArtsStudio:instance:listDrivers
  - DataArtsStudio:instance:listTags
  - DataArtsStudio:workspace:listTags

**Table 3-186** Actions supported by DataArts Studio

| Action                        | Description                                    | Access Level | Resource Type (*: Required) | Condition Key                                 | Alias                                                                  |
|-------------------------------|------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------|
| DataArtsStudio:workspace:list | Grants the permission to query all workspaces. | List         | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>• dgc:workspace:list</li> </ul> |
|                               |                                                |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                                                        |

| Action                            | Description                                           | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                     | Alias                                                                |
|-----------------------------------|-------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| DataArtsStudio:workspace:create   | Grants the permission to create a workspace.          | Write        | workspace *                 | -                                                                                                                                 | -                                                                    |
|                                   |                                                       |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                      |
|                                   |                                                       |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                                                                      |
| DataArtsStudio:workspace:get      | Grants the permission to query workspace information. | Read         | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                                                                    |
|                                   |                                                       |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                      |
| DataArtsStudio:workspace:freeze   | Grants the permission to freeze a workspace.          | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                                                                    |
|                                   |                                                       |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                      |
| DataArtsStudio:workspace:unfreeze | Grants the permissions to unfreeze a workspace.       | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                                                                    |
|                                   |                                                       |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                      |
| DataArtsStudio:workspace:update   | Grants the permission to update a workspace.          | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                                                                    |
|                                   |                                                       |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                      |
| DataArtsStudio:instance:list      | Grants the permission to query all instances.         | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | <ul style="list-style-type: none"> <li>dgc:workspace:list</li> </ul> |
| DataArtsStudio:instance:create    | Grants the permission to create an instance.          | Write        | instance *                  | -                                                                                                                                 | -                                                                    |

| Action                               | Description                                              | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                         | Alias |
|--------------------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                      |                                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| DataArtsStudio:instance:get          | Grants the permission to query an instance.              | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -     |
| DataArtsStudio:instance:resize       | Grants the permission to change instance specifications. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -     |
| DataArtsStudio:instance:listDrivers  | Grants the permission to query all driver files.         | List         | -                           | -                                                                                                                                     | -     |
| DataArtsStudio:instance:uploadDriver | Grants the permission to upload a driver file.           | Write        | -                           | -                                                                                                                                     | -     |
| DataArtsStudio:instance:deleteDriver | Grants the permission to delete a driver file.           | Write        | -                           | -                                                                                                                                     | -     |
| DataArtsStudio:workspace:delete      | Grants the permission to delete a workspace.             | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -     |
|                                      |                                                          |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         |       |
| DataArtsStudio:instance:getAgency    | Grants the permission to query an agency.                | Read         | -                           | -                                                                                                                                     | -     |
| DataArtsStudio:instance:createAgency | Grants the permission to create an agency.               | Write        | -                           | -                                                                                                                                     | -     |

| Action                                       | Description                                                        | Access Level | Resource Type (*: Required) | Condition Key                                 | Alias |
|----------------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| DataArtsStudio:instance:delete               | Grants the permission to delete an instance.                       | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:instance:migrateBusinessModel | Grants the permission to change the business model of an instance. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:instance:operate              | Grants the permission to operate the resources of an instance.     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:workspace:operate             | Grants the permission to operate the resources in a workspace.     | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                              |                                                                    |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| DataArtsStudio:instance:createRole           | Grants the permission to create a custom role.                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:instance:listRoles            | Grants the permission to query custom roles.                       | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:instance:getRoleType          | Grants the permission to query the type of a custom role.          | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:instance:getRole              | Grants the permission to query a custom role.                      | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                                            | Description                                                             | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                              | Alias |
|---------------------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| DataArtsStudio:instance:updateRole                | Grants the permission to update a custom role.                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                              | -     |
| DataArtsStudio:instance:deleteRole                | Grants the permission to delete a custom role.                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                              | -     |
| DataArtsStudio:instance:tagResource               | Grants the permission to add an instance tag.                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                              | -     |
|                                                   |                                                                         |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>                          |       |
| DataArtsStudio:instance:unTagResource             | Grants the permission to delete an instance tag.                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                              | -     |
|                                                   |                                                                         |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>                          |       |
| DataArtsStudio:instance:listIncrementalPackages   | Grants the permission to query all incremental packages.                | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                              | -     |
| DataArtsStudio:workspace:createIncrementalPackage | Grants the permission to create an incremental package for a workspace. | Write        | workspace *                 | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">DataArtsStudio:EnablePublicAccess</a></li> </ul> | -     |
|                                                   |                                                                         |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                              |       |
| DataArtsStudio:workspace:tagResource              | Grants the permission to add a tag to a workspace.                      | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                              | -     |



| Action                                           | Description                                                             | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                     | Alias |
|--------------------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
|                                                  |                                                                         |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                                                  |                                                                         |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| DataArtsStudio:workspace:unTagResource           | Grants the permission to delete a tag from a workspace.                 | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                                  |                                                                         |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                                                  |                                                                         |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| DataArtsStudio:instance:createIncrementalPackage | Grants the permission to create an incremental package for an instance. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| DataArtsStudio:instance:listTags                 | Grants the permission to query the tags of all instances.               | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| DataArtsStudio:workspace:listTags                | Grants the permission to query the tags of all workspaces.              | List         | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                                  |                                                                         |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
| DataArtsStudio:instance:listTagsForResource      | Grants the permission to query the tags of an instance.                 | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |

| Action                                                     | Description                                                                                   | Access Level | Resource Type (*: Required) | Condition Key                                 | Alias |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| DataArtsStudio:workspace:listTagsForResource               | Grants the permission to query the tags of a workspace.                                       | List         | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                                            |                                                                                               |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| DataArtsStudio:workspace:updateDataServiceApiQuota         | Grants the permission to update the DataArts DataService API quota of a workspace.            | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                                            |                                                                                               |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| DataArtsStudio:workspace:executeDataServiceInstanceAction  | Grants the permission to run commands to perform operations on DataArts DataService clusters. | Write        | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                                            |                                                                                               |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| DataArtsStudio:instance:configureDataSecurityAdministrator | Grants the permission to configure the data security administrator.                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:instance:listResourcesByTag                 | Grants the permission to filter instances by tag.                                             | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| DataArtsStudio:workspace:listResourcesByTag                | Grants the permission to filter workspaces by tag.                                            | List         | workspace *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                                            |                                                                                               |              | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |

Each API of DataArts Studio usually supports one or more actions. [Table 3-187](#) lists the actions and dependencies supported by DataArts Studio APIs.

**Table 3-187** Actions and dependencies supported by DataArts Studio APIs

| API                                                          | Action                          | Dependency |
|--------------------------------------------------------------|---------------------------------|------------|
| GET /v1/{project_id}/workspaces/{instance_id}                | DataArtsStudio:workspace:list   | -          |
| POST /v1/{project_id}/workspaces/{instance_id}               | DataArtsStudio:workspace:create | -          |
| GET /v1/{project_id}/workspaces/{instance_id}/{workspace_id} | DataArtsStudio:workspace:get    | -          |
| POST /v1/{project_id}/change-resource                        | DataArtsStudio:instance:resize  | -          |
| GET /v1/{project_id}/instances                               | DataArtsStudio:instance:list    | -          |
| POST /v1/{project_id}/instances/onekey-purchase              | DataArtsStudio:instance:create  | -          |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-188](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DataArts Studio.

**Table 3-188** Resource types supported by DataArts Studio

| Resource Type | URN                                                                         |
|---------------|-----------------------------------------------------------------------------|
| workspace     | DataArtsStudio:<region>:<account-id>:workspace:<instance-id>/<workspace-id> |

| Resource Type | URN                                                         |
|---------------|-------------------------------------------------------------|
| instance      | DataArtsStudio:<region>:<account-id>:instance:<instance-id> |

## Conditions

### About condition keys

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- Condition keys are the key values in the Condition element of an identity policy statement. They are classified into global condition keys and service-specific condition keys based on the application scope.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, dataarts studio:) apply only to operations of the specific service. For details, see [Table 3-189](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- An operator, a condition key, and a condition value together constitute a complete condition statement. An identity policy becomes in effect only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by DataArts Studio

The following table lists the condition keys that you can define in custom identity policies for DataArts Studio. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-189** Service-specific condition keys supported by DataArts Studio

| Service-specific Condition Key    | Type    | Single-valued/<br>Multivalued | Description                                         |
|-----------------------------------|---------|-------------------------------|-----------------------------------------------------|
| DataArtsStudio:EnablePublicAccess | boolean | Single-valued                 | Whether the service is accessible over the Internet |

### 3.9.3 Data Lake Insight(DLI)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted IAM identity permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences Between IAM Policies and Organizations SCPs?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP policy, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DLI, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.

- If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
- If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DLI, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization.

For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in custom identity policies for DLI.

**Table 3-190** Actions supported by DLI

| Action              | Description                                       | Access Level          | Resource Type (*: required) | Condition Key |
|---------------------|---------------------------------------------------|-----------------------|-----------------------------|---------------|
| dli::operateAuth    | Grants the permission to manage DLI permissions.  | permission_management | -                           | -             |
| dli::listAuth       | Grants the permission to query DLI permissions.   | list                  | -                           | -             |
| dli:variable:list   | Grants the permission to list global variables.   | list                  | variable *                  | -             |
| dli:variable:create | Grants the permission to create global variables. | write                 | variable *                  | -             |
| dli:variable:update | Grants the permission to update global variables. | write                 | variable *                  | -             |
| dli:variable:delete | Grants the permission to delete global variables. | write                 | variable *                  | -             |
| dli:catalog:list    | Grants the permission to list data catalogs.      | list                  | -                           | -             |

| Action           | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                    |
|------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| dli:catalog:bind | Grants the permission to bind data catalogs.         | write        | -                           | -                                                                                                                                |
| dli:catalog:get  | Grants the permission to query data catalog details. | read         | -                           | -                                                                                                                                |
| dli:queue:list   | Grants the permission to list queues.                | list         | queue *                     | -                                                                                                                                |
|                  |                                                      |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                                |
| dli:queue:create | Grants the permission to create queues.              | write        | queue *                     | -                                                                                                                                |
|                  |                                                      |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:get    | Grants the permission to query queue details.        | read         | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:queue:update | Grants the permission to update queues.              | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:queue:delete | Grants the permission to delete queues.              | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:queue:scale  | Grants the permission to scale out/in a queue.       | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |

| Action                    | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                  |
|---------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|
| dli:queue:checkConnection | Grants the permission to test the connectivity of an address.         | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:getConnection   | Grants the permission to query connectivity results.                  | read         | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:listPlans       | Grants the permission to list scheduled scaling plans of a queue.     | list         | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:createPlan      | Grants the permission to create scheduled scaling plans for a queue.  | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:deletePlan      | Grants the permission to delete scheduled scaling plans from a queue. | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:updatePlan      | Grants the permission to update scheduled scaling plans for a queue.  | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:createProperty  | Grants the permission to create configurations for a queue.           | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:listProperties  | Grants the permission to list queue configurations.                   | list         | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |



| Action                   | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                  |
|--------------------------|--------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|
| dli:queue:updateProperty | Grants the permission to update configurations for a queue.  | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:deleteProperty | Grants the permission to delete configurations from a queue. | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:jobs:list            | Grants the permission to list jobs.                          | list         | jobs *                      | -                                                                                                              |
|                          |                                                              |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>              |
| dli:queue:submitJob      | Grants the permission to submit jobs on a queue.             | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:jobs:get             | Grants the permission to query job details.                  | read         | jobs *                      | g:ResourceTag/<tag-key>                                                                                        |
| dli:table:select         | Grants the permission to query tables.                       | read         | table *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:table:insertInto     | Grants the permission to insert table data.                  | write        | table *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:queue:cancelJob      | Grants the permission to cancel jobs on a queue.             | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |

| Action                        | Description                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                    |
|-------------------------------|-----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| dli:jobs:exportResult         | Grants the permission to export job results.              | read         | jobs *                      | g:ResourceTag/<tag-key>                                                                                                          |
| dli::checkSql                 | Grants the permission to verify the SQL syntax.           | write        | -                           | -                                                                                                                                |
| dli:database:list             | Grants the permission to list databases.                  | list         | database *                  | -                                                                                                                                |
|                               |                                                           |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                                |
| dli:database:create           | Grants the permission to create databases.                | write        | database *                  | -                                                                                                                                |
|                               |                                                           |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:database:update           | Grants the permission to update databases.                | write        | database *                  | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:database:delete           | Grants the permission to delete databases.                | write        | database *                  | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:database:displayAllTables | Grant the permission to display all tables in a database. | list         | database *                  | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:database:createTable      | Grants the permission to create tables in a database.     | write        | database *                  | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |

| Action                   | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                  |
|--------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|
| dli:table:update         | Grants the permission to update tables.                     | write        | table *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:table:describe       | Grants the permission to display the table structure.       | read         | table *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:table:delete         | Grants the permission to delete tables.                     | write        | table *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:table:showPartitions | Grants the permission to display all partitions of a table. | read         | table *                     | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:sqldefendrule:create | Grants the permission to create SQL inspection rules.       | write        | -                           | -                                                                                                              |
| dli:sqldefendrule:list   | Grants the permission to list SQL inspection rules.         | list         | -                           | -                                                                                                              |
| dli:sqldefendrule:update | Grants the permission to update SQL inspection rules.       | write        | -                           | -                                                                                                              |
| dli:sqldefendrule:delete | Grants the permission to delete SQL inspection rules.       | write        | -                           | -                                                                                                              |

| Action                | Description                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                     |
|-----------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------|
| dli:sqldefendrule:get | Grants the permission to query details about SQL inspection rules. | read         | -                           | -                                                                                                 |
| dli:resource:create   | Grants the permission to create resource packages.                 | write        | resource *                  | -                                                                                                 |
|                       |                                                                    |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |
| dli:resource:get      | Grants the permission to query resource package details.           | read         | resource *                  | g:ResourceTag/<tag-key>                                                                           |
| dli:resource:delete   | Grants the permission to delete resource packages.                 | write        | resource *                  | g:ResourceTag/<tag-key>                                                                           |
| dli:resource:list     | Grants the permission to list resource packages.                   | list         | resource *                  | -                                                                                                 |
|                       |                                                                    |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |
| dli:resource:update   | Grants the permission to update resource packages.                 | write        | resource *                  | g:ResourceTag/<tag-key>                                                                           |
| dli:jobs:update       | Grants the permission to update jobs.                              | write        | jobs *                      | g:ResourceTag/<tag-key>                                                                           |
| dli:jobs:delete       | Grants the permission to delete jobs.                              | write        | jobs *                      | g:ResourceTag/<tag-key>                                                                           |
| dli:jobs:create       | Grants the permission to create jobs.                              | write        | jobs *                      | -                                                                                                 |
|                       |                                                                    |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |

| Action                     | Description                                                            | Access Level | Resource Type (*: required) | Condition Key            |
|----------------------------|------------------------------------------------------------------------|--------------|-----------------------------|--------------------------|
| dli:jobs:startFlinkJob     | Grants the permission to start a job.                                  | write        | jobs *                      | g:ResourceTag /<tag-key> |
| dli:jobs:stopFlinkJob      | Grants the permission to stop a job.                                   | write        | jobs *                      | g:ResourceTag /<tag-key> |
| dli:jobs:export            | Grants the permission to export jobs.                                  | write        | jobs *                      | g:ResourceTag /<tag-key> |
| dli::createEdgeChannel     | Grants the permission to create IEF message channels.                  | write        | -                           | -                        |
| dli::reportEdgeJob         | Grants the permission to report statuses of Flink edge jobs.           | write        | -                           | -                        |
| dli::callbackEdgeJobAction | Grants the permission to call back action statuses of Flink edge jobs. | write        | -                           | -                        |
| dli::createEdgeSystemEvent | Grants the permission to report IEF system events.                     | write        | -                           | -                        |
| dli:template:list          | Grants the permission to list templates.                               | list         | template *                  | -                        |
| dli:template:create        | Grants the permission to create templates.                             | write        | template *                  | -                        |
| dli:template:update        | Grants the permission to update templates.                             | write        | template *                  | -                        |

| Action                                           | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                    |
|--------------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| dli:template:delete                              | Grants the permission to delete templates.                             | write        | template *                  | -                                                                                                                                |
| dli:template:get                                 | Grants the permission to query template details.                       | read         | template *                  | -                                                                                                                                |
| dli:elasticsearchresourcepool:resourceManagement | Grants the permission to manage resources to an elastic resource pool. | write        | elasticsearchresourcepool * | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:elasticsearchresourcepool:list               | Grants the permission to list elastic resource pools.                  | list         | elasticsearchresourcepool * | -                                                                                                                                |
|                                                  |                                                                        |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                                |
| dli:elasticsearchresourcepool:create             | Grants the permission to create elastic resource pools.                | write        | elasticsearchresourcepool * | -                                                                                                                                |
|                                                  |                                                                        |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:elasticsearchresourcepool:update             | Grants the permission to update elastic resource pools.                | write        | elasticsearchresourcepool * | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |
| dli:elasticsearchresourcepool:delete             | Grants the permission to delete elastic resource pools.                | write        | elasticsearchresourcepool * | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul>                   |

| Action                        | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                  |
|-------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|
| dli:elasticresourcepool:scale | Grants the permission to scale out/in an elastic resource pool.                 | list         | elasticresourcepool *       | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli::createLakehouse          | Grants the permission to create lakehouses.                                     | write        | -                           | -                                                                                                              |
| dli::getLakehouse             | Grants the permission to query lakehouses.                                      | read         | -                           | -                                                                                                              |
| dli:connection:list           | Grants the permission to list basic datasource connections.                     | list         | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>              |
| dli:connection:create         | Grants the permission to create basic datasource connections.                   | write        | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>              |
| dli:connection:get            | Grants the permission to query basic datasource connections.                    | read         | -                           | -                                                                                                              |
| dli:connection:delete         | Grants the permission to delete basic datasource connections.                   | write        | -                           | -                                                                                                              |
| dli:edsconnection:get         | Grants the permission to query details about an enhanced datasource connection. | read         | edsconnection *             | g:ResourceTag/<tag-key>                                                                                        |

| Action                        | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                        |
|-------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------|
| dli:edsconnection:update      | Grants the permission to update enhanced datasource connections.                | write        | edsconnection *             | g:ResourceTag /<tag-key>                                                                                             |
| dli:edsconnection:delete      | Grants the permission to delete enhanced datasource connections.                | write        | edsconnection *             | g:ResourceTag /<tag-key>                                                                                             |
| dli:edsconnection:list        | Grants the permission to list enhanced datasource connections.                  | list         | edsconnection *             | -                                                                                                                    |
|                               |                                                                                 |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>                    |
| dli:edsconnection:create      | Grants the permission to create enhanced datasource connections.                | write        | edsconnection *             | -                                                                                                                    |
|                               |                                                                                 |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> <li>dli:VpcId</li> </ul> |
| dli:edsconnection:unbindQueue | Grants the permission to unbind an enhanced datasource connection from a queue. | write        | edsconnection *             | g:ResourceTag /<tag-key>                                                                                             |
| dli:edsconnection:bindQueue   | Grants the permission to bind an enhanced datasource connection to a queue.     | write        | edsconnection *             | g:ResourceTag /<tag-key>                                                                                             |
| dli:datasourceauth:list       | Grants the permission to list datasource authentication connections.            | list         | datasourceauth *            | -                                                                                                                    |



| Action                         | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                   |
|--------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------|
| dli:datasourceauth:update      | Grants the permission to update security authentication information.         | write        | datasourceauth *            | -                                                                                                               |
| dli:datasourceauth:create      | Grants the permission to create security authentication information.         | write        | datasourceauth *            | -                                                                                                               |
| dli:datasourceauth:delete      | Grants the permission to delete security authentication information.         | write        | datasourceauth *            | -                                                                                                               |
| dli:edsconnection:deleteRoute  | Grants the permission to delete routes from enhanced datasource connections. | write        | edsconnection *             | g:ResourceTag /<tag-key>                                                                                        |
| dli:edsconnection:createRoute  | Grants the permission to create routes for enhanced datasource connections.  | write        | edsconnection *             | g:ResourceTag /<tag-key>                                                                                        |
| dli::getQuota                  | Grants the permission to query quotas.                                       | read         | -                           | -                                                                                                               |
| dli:queue:restart              | Grants the permission to restart a queue.                                    | write        | queue *                     | <ul style="list-style-type: none"> <li>g:ResourceTag /&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
| dli:table:insertOverwriteTable | Grants the permission to overwrite data to a table.                          | write        | table *                     | <ul style="list-style-type: none"> <li>g:ResourceTag /&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |

| Action                  | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                  |
|-------------------------|--------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|
| dli:catalog:unbind      | Grants the permission to unbind data catalogs.   | write        | -                           | -                                                                                                              |
| dli::listTags           | Grants the permission to list tags.              | list         | -                           | -                                                                                                              |
| dli::listResourcesByTag | Grants the permission to query resources by tag. | list         | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>              |
| dli::unTagResource      | Grants the permission to delete tags.            | tagging      | queue                       | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> |
|                         |                                                  |              | resource                    | g:ResourceTag/<tag-key>                                                                                        |
|                         |                                                  |              | database                    | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> |
|                         |                                                  |              | elasticresource-pool        | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> |
|                         |                                                  |              | edsconnection               | g:ResourceTag/<tag-key>                                                                                        |
|                         |                                                  |              | jobs                        | g:ResourceTag/<tag-key>                                                                                        |
|                         |                                                  |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul>              |

| Action                   | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                  |
|--------------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|
| dli::listTagsForResource | Grants the permission to query the tags of a specified resource. | list         | queue                       | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> |
|                          |                                                                  |              | resource                    | g:ResourceTag/<tag-key>                                                                                        |
|                          |                                                                  |              | database                    | <ul style="list-style-type: none"> <li>g:EnterpriseProjectId</li> <li>g:ResourceTag/&lt;tag-key&gt;</li> </ul> |
|                          |                                                                  |              | elasticresource-pool        | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> |
|                          |                                                                  |              | edsconnection               | g:ResourceTag/<tag-key>                                                                                        |
|                          |                                                                  |              | jobs                        | g:ResourceTag/<tag-key>                                                                                        |
| dli::createDownloader    | Grants the permission to create download tasks.                  | write        | -                           | -                                                                                                              |

Each API of DLI usually supports one or more actions. [Table 3-191](#) lists the actions and dependencies supported by DLI APIs.

**Table 3-191** Actions and dependencies supported by open DLI APIs

| API                                                                        | Action           | Dependency |
|----------------------------------------------------------------------------|------------------|------------|
| PUT /v1.0/{project_id}/queues/user-authorization                           | dli::operateAuth | -          |
| PUT /v1.0/{project_id}/user-authorization                                  | dli::operateAuth | -          |
| GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/users | dli::listAuth    | -          |

| API                                                                                    | Action                    | Dependency         |
|----------------------------------------------------------------------------------------|---------------------------|--------------------|
| GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/users/{user_name} | dli::listAuth             | -                  |
| GET /v1.0/{project_id}/databases/{database_name}/users                                 | dli::listAuth             | -                  |
| GET /v1.0/{project_id}/queues/{queue_name}/users                                       | dli::listAuth             | -                  |
| GET /v1.0/{project_id}/authorization/privileges                                        | dli::listAuth             | -                  |
| PUT /v1.0/{project_id}/authorization                                                   | dli::operateAuth          | -                  |
| GET /v1.0/{project_id}/variables                                                       | dli:variable:list         | -                  |
| POST /v1.0/{project_id}/variables                                                      | dli:variable:create       | -                  |
| PUT /v1.0/{project_id}/variables/{var_name}                                            | dli:variable:update       | -                  |
| DELETE /v1.0/{project_id}/variables/{var_name}                                         | dli:variable:delete       | -                  |
| GET /v3/{project_id}/catalogs                                                          | dli:catalog:list          | -                  |
| POST /v3/{project_id}/catalogs/action                                                  | dli:catalog:bind          | dli:catalog:unbind |
| GET /v3/{project_id}/catalogs/{catalog_name}                                           | dli:catalog:get           | -                  |
| GET /v1.0/{project_id}/queues                                                          | dli:queue:list            | -                  |
| POST /v1.0/{project_id}/queues                                                         | dli:queue:create          | -                  |
| GET /v1.0/{project_id}/queues/{queue_name}                                             | dli:queue:get             | -                  |
| PUT /v1.0/{project_id}/queues/{queue_name}                                             | dli:queue:update          | -                  |
| DELETE /v1.0/{project_id}/queues/{queue_name}                                          | dli:queue:delete          | -                  |
| PUT /v1.0/{project_id}/queues/{queue_name}/action                                      | dli:queue:scale           | dli:queue:restart  |
| POST /v1.0/{project_id}/queues/{queue_name}/connection-test                            | dli:queue:checkConnection | -                  |
| GET /v1.0/{project_id}/queues/{queue_name}/connection-test/{task_id}                   | dli:queue:getConnection   | -                  |
| GET /v1/{project_id}/queues/{queue_name}/plans                                         | dli:queue:listPlans       | -                  |

| API                                                          | Action                   | Dependency |
|--------------------------------------------------------------|--------------------------|------------|
| POST /v1/{project_id}/queues/{queue_name}/plans              | dli:queue:createPlan     | -          |
| POST /v1/{project_id}/queues/{queue_name}/plans/batch-delete | dli:queue:deletePlan     | -          |
| PUT /v1.0/{project_id}/queues/{queue_name}                   | dli:queue:updatePlan     | -          |
| DELETE /v1/{project_id}/queues/{queue_name}/plans/{plan_id}  | dli:queue:deletePlan     | -          |
| POST /v3/{project_id}/queues/{queue_name}/properties         | dli:queue:createProperty | -          |
| GET /v3/{project_id}/queues/{queue_name}/properties          | dli:queue:listProperties | -          |
| PUT /v3/{project_id}/queues/{queue_name}/properties          | dli:queue:updateProperty | -          |
| DELETE /v3/{project_id}/queues/{queue_name}/properties       | dli:queue:deleteProperty | -          |
| GET /v1.0/{project_id}/jobs                                  | dli:jobs:list            | -          |
| POST /v1.0/{project_id}/jobs/submit-job                      | dli:queue:submitJob      | -          |
| GET /v1.0/{project_id}/jobs/{job_id}/status                  | dli:jobs:get             | -          |
| GET /v1.0/{project_id}/jobs/{job_id}/detail                  | dli:jobs:get             | -          |
| DELETE /v1.0/{project_id}/jobs/{job_id}                      | dli:queue:cancelJob      | -          |
| GET /v1.0/{project_id}/jobs/{job_id}/preview                 | dli:jobs:get             | -          |
| POST /v1.0/{project_id}/jobs/check-sql                       | dli::checkSql            | -          |
| GET /v1/{project_id}/jobs/{job_id}/progress                  | dli:jobs:get             | -          |
| POST /v1/{project_id}/sql-defend-rules                       | dli:sqldefendrule:create | -          |
| GET /v1/{project_id}/sql-defend-rules                        | dli:sqldefendrule:list   | -          |
| PUT /v1/{project_id}/sql-defend-rules/{rule_id}              | dli:sqldefendrule:update | -          |

| API                                                              | Action                   | Dependency          |
|------------------------------------------------------------------|--------------------------|---------------------|
| DELETE /v1/{project_id}/sql-defend-rules/{rule_id}               | dli:sqldefendrule:delete | -                   |
| GET /v1/{project_id}/sql-defend-rules/{rule_id}                  | dli:sqldefendrule:get    | -                   |
| POST /v1.0/{project_id}/streaming/jobs/{job_id}/import-savepoint | dli:jobs:update          | -                   |
| POST /v1.0/{project_id}/streaming/jobs/{job_id}/savepoint        | dli:jobs:update          | -                   |
| GET /v1.0/{project_id}/streaming/jobs/{job_id}                   | dli:jobs:get             | -                   |
| DELETE /v1.0/{project_id}/streaming/jobs/{job_id}                | dli:jobs:delete          | -                   |
| GET /v1.0/{project_id}/streaming/jobs                            | dli:jobs:list            | -                   |
| POST /v1.0/{project_id}/streaming/sql-jobs                       | dli:jobs:create          | -                   |
| PUT /v1.0/{project_id}/streaming/sql-jobs/{job_id}               | dli:jobs:update          | -                   |
| POST /v1.0/{project_id}/streaming/flink-jobs                     | dli:jobs:create          | -                   |
| PUT /v1.0/{project_id}/streaming/flink-jobs/{job_id}             | dli:jobs:update          | -                   |
| POST /v1.0/{project_id}/streaming/jobs/run                       | dli:jobs:startFlinkJob   | dli:queue:submitJob |
| POST /v1.0/{project_id}/streaming/jobs/stop                      | dli:jobs:stopFlinkJob    | dli:queue:cancelJob |
| POST /v1.0/{project_id}/streaming/jobs/delete                    | dli:jobs:delete          | -                   |
| GET /v1.0/{project_id}/streaming/jobs/{job_id}/execute-graph     | dli:jobs:get             | -                   |
| POST /v1.0/{project_id}/streaming/jobs/export                    | dli:jobs:export          | -                   |
| POST /v1.0/{project_id}/streaming/jobs/import                    | dli:jobs:create          | -                   |
| POST /v3/{project_id}/streaming/jobs/{job_id}/gen-graph          | dli:jobs:get             | -                   |
| GET /v1.0/{project_id}/streaming/job-templates                   | dli:template:list        | -                   |

| API                                                                                          | Action                                      | Dependency |
|----------------------------------------------------------------------------------------------|---------------------------------------------|------------|
| POST /v1.0/{project_id}/streaming/job-templates                                              | dli:template:create                         | -          |
| PUT /v1.0/{project_id}/streaming/job-templates/{template_id}                                 | dli:template:update                         | -          |
| DELETE /v1.0/{project_id}/streaming/job-templates/{template_id}                              | dli:template:delete                         | -          |
| POST /v1.0/{project_id}/sqls                                                                 | dli:template:create                         | -          |
| GET /v1.0/{project_id}/sqls                                                                  | dli:template:list                           | -          |
| GET /v1.0/{project_id}/sqls/sample                                                           | dli:template:list                           | -          |
| PUT /v1.0/{project_id}/sqls/{template_id}                                                    | dli:template:update                         | -          |
| POST /v1.0/{project_id}/sqls-deletion                                                        | dli:template:delete                         | -          |
| POST /v3/{project_id}/templates                                                              | dli:template:create                         | -          |
| GET /v3/{project_id}/templates                                                               | dli:template:list                           | -          |
| PUT /v3/{project_id}/templates/{template_id}                                                 | dli:template:update                         | -          |
| GET /v3/{project_id}/templates/{template_id}                                                 | dli:template:get                            | -          |
| GET /v2.0/{project_id}/batches                                                               | dli:jobs:list                               | -          |
| POST /v2.0/{project_id}/batches                                                              | dli:queue:submitJob                         | -          |
| GET /v2.0/{project_id}/batches/{batch_id}                                                    | dli:jobs:get                                | -          |
| DELETE /v2.0/{project_id}/batches/{batch_id}                                                 | dli:queue:cancelJob                         | -          |
| GET /v2.0/{project_id}/batches/{batch_id}/log                                                | dli:jobs:get                                | -          |
| GET /v2.0/{project_id}/batches/{batch_id}/state                                              | dli:jobs:get                                | -          |
| POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/notebook/action    | dli:elasticresource-pool:resourceManagement | -          |
| POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/notebook/instances | dli:elasticresource-pool:resourceManagement | -          |

| API                                                                                          | Action                                      | Dependency                                                                                   |
|----------------------------------------------------------------------------------------------|---------------------------------------------|----------------------------------------------------------------------------------------------|
| GET /v3/{project_id}/elastic-resource-pools                                                  | dli:elasticresource-pool:list               | -                                                                                            |
| POST /v3/{project_id}/elastic-resource-pools                                                 | dli:elasticresource-pool:create             | -                                                                                            |
| PUT /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}                     | dli:elasticresource-pool:update             | -                                                                                            |
| DELETE /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}                  | dli:elasticresource-pool:delete             | -                                                                                            |
| GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues              | dli:elasticresource-pool:resourceManagement | -                                                                                            |
| POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues             | dli:elasticresource-pool:resourceManagement | <ul style="list-style-type: none"> <li>dli:queue:create</li> <li>dli:queue:delete</li> </ul> |
| PUT /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues/{queue_name} | dli:elasticresource-pool:resourceManagement | -                                                                                            |
| GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/scale-records       | dli:elasticresource-pool:scale              | -                                                                                            |
| POST /v3/{project_id}/orders/elastic-resource-pools                                          | dli:elasticresource-pool:create             | -                                                                                            |
| POST /v3/{project_id}/orders/elastic-resource-pools/specification-change                     | dli:elasticresource-pool:scale              | -                                                                                            |
| POST /v3/{project_id}/lakehouse                                                              | dli::createLakehouse                        | -                                                                                            |
| GET /v3/{project_id}/lakehouse                                                               | dli::getLakehouse                           | -                                                                                            |
| GET /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}                       | dli:edsconnection:get                       | -                                                                                            |
| PUT /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}                       | dli:edsconnection:update                    | -                                                                                            |
| DELETE /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}                    | dli:edsconnection:delete                    | -                                                                                            |
| GET /v2.0/{project_id}/datasource/enhanced-connections                                       | dli:edsconnection:list                      | -                                                                                            |



| API                                                                                        | Action                        | Dependency |
|--------------------------------------------------------------------------------------------|-------------------------------|------------|
| POST /v2.0/{project_id}/datasource/enhanced-connections                                    | dli:edsconnection:create      | -          |
| POST /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/disassociate-queue | dli:edsconnection:unbindQueue | -          |
| POST /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/associate-queue    | dli:edsconnection:bindQueue   | -          |
| GET /v2.0/{project_id}/datasource/enhanced-connections/{connection_id}/privileges          | dli::listAuth                 | -          |
| GET /v3/{project_id}/datasource/auth-infos                                                 | dli:datasourceauth:list       | -          |
| PUT /v3/{project_id}/datasource/auth-infos                                                 | dli:datasourceauth:update     | -          |
| POST /v3/{project_id}/datasource/auth-infos                                                | dli:datasourceauth:create     | -          |
| DELETE /v3/{project_id}/datasource/auth-infos/{auth_info_name}                             | dli:datasourceauth:delete     | -          |
| POST /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes               | dli:edsconnection:deleteRoute | -          |
| DELETE /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes/{name}      | dli:edsconnection:createRoute | -          |
| GET /v3/{project_id}/quotas                                                                | dli::getQuota                 | -          |
| GET /v3/{project_id}/datasource/auth-infos                                                 | dli:datasourceauth:list       | -          |
| PUT /v3/{project_id}/datasource/auth-infos                                                 | dli:datasourceauth:update     | -          |
| POST /v3/{project_id}/datasource/auth-infos                                                | dli:datasourceauth:create     | -          |
| DELETE /v3/{project_id}/datasource/auth-infos/{auth_info_name}                             | dli:datasourceauth:delete     | -          |
| POST /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes               | dli:edsconnection:createRoute | -          |

| API                                                                                   | Action                         | Dependency |
|---------------------------------------------------------------------------------------|--------------------------------|------------|
| DELETE /v3/{project_id}/datasource/enhanced-connections/{connection_id}/routes/{name} | dli::edsconnection:deleteRoute | -          |
| GET /v3/{project_id}/{resource_type}/tags                                             | dli::listTags                  | -          |
| POST /v3/{project_id}/{resource_type}/resource-instances/filter                       | dli::listResourcesBy-Tag       | -          |
| POST /v3/{project_id}/{resource_type}/resource-instances/count                        | dli::listResourcesBy-Tag       | -          |
| POST /v3/{project_id}/{resource_type}/{resource_id}/tags/delete                       | dli::unTagResource             | -          |
| GET /v3/{project_id}/{resource_type}/{resource_id}/tags                               | dli::listTagsForResource       | -          |

**Table 3-192** Actions and dependencies supported by DLI console APIs

| API                                                   | Action              | Dependency |
|-------------------------------------------------------|---------------------|------------|
| GET /v1.0/{project_id}/logs/transfer                  | dli::getLogTransfer | -          |
| POST /v1.0/{project_id}/logs/history                  | dli::getLog         | -          |
| POST /v1.0/{project_id}/logs/runtime                  | dli::getLog         | -          |
| GET /v1.0/{project_id}/logs/pods                      | dli::getLog         | -          |
| GET /v1.0/{project_id}/logs/pods/{pod_name}           | dli::getLog         | -          |
| PUT /v1.0/{project_id}/databases/{database_name}/name | dli:database:update | -          |
| POST /v1/{project_id}/streaming/jobs/check            | dli:jobs:check      | -          |
| POST /v1/{project_id}/streaming/sql/validate          | dli::checkSql       | -          |
| GET /v1/{project_id}/streaming/jobs/{job_id}/log      | dli:jobs:get        | -          |

| API                                                                                                             | Action                 | Dependency |
|-----------------------------------------------------------------------------------------------------------------|------------------------|------------|
| GET /v1/{project_id}/streaming/jobs/{job_id}/log/{tm_id}                                                        | dli:jobs:get           | -          |
| GET /v1/{project_id}/streaming/jobs/{job_id}/submitlog                                                          | dli:jobs:get           | -          |
| POST /v1/{project_id}/streaming/templates/check                                                                 | dli:template:check     | -          |
| GET /v1.0/{project_id}/databases/{database_name}/projects                                                       | dli::listAuth          | -          |
| GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/projects                                   | dli::listAuth          | -          |
| GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/projects/{projectId}                       | dli::listAuth          | -          |
| GET /v1.0/{project_id}/databases/{database_name}/projects/{projectId}                                           | dli::listAuth          | -          |
| GET /v1.0/{project_id}/databases/{database_name}/tables/{table_name}/columns/{column_name}/projects/{projectId} | dli::listAuth          | -          |
| POST /v1.0/{project_id}/logs/transfer                                                                           | dli::createLogTransfer | -          |
| POST /v1.0/{project_id}/orders/queues                                                                           | dli:queue:create       | -          |
| PUT /v1.0/{project_id}/orders/queues                                                                            | dli:queue:scale        | -          |
| PUT /v3/{project_id}/queues/{queue_name}/scale-range                                                            | dli:queue:scale        | -          |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-193](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DLI.

**Table 3-193** Resource types supported by DLI

| Resource Type       | URN                                                                                  |
|---------------------|--------------------------------------------------------------------------------------|
| variable            | dli:<region>:<account-id>:variable:<variable-name-with-prefix>                       |
| queue               | dli:<region>:<account-id>:queue:<queue-name-with-prefix>                             |
| jobs                | dli:<region>:<account-id>:jobs:<job-id-with-prefix>                                  |
| table               | dli:<region>:<account-id>:table:<table-name-with-prefix>                             |
| database            | dli:<region>:<account-id>:database:<database-name-with-prefix>                       |
| resource            | dli:<region>:<account-id>:resource:<resource-name-with-prefix>                       |
| template            | dli:<region>:<account-id>:template:<template-name-with-prefix>                       |
| elasticresourcepool | dli:<region>:<account-id>:elasticresourcepool:<elasticresourcepool-name-with-prefix> |
| edsconnection       | dli:<region>:<account-id>:edsconnection:<edsconnection-id-with-prefix>               |
| datasourceauth      | dli:<region>:<account-id>:datasourceauth:<datasourceauth-name-with-prefix>           |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name as the prefix, for example, **dli:**) apply only to DLI operations. For details, see [Table 3-194](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have

multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.

- An operator, a condition key, and a condition value together constitute a complete condition statement. An identity policy becomes in effect only when its request conditions are met. For supported condition operators, see [Condition operators](#).

The following table lists the condition keys that you can define in custom identity policies for DLI. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-194** Service-specific condition keys supported by DLI

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                           |
|--------------------------------|--------|-------------------------------|---------------------------------------|
| <code>dli:VpcId</code>         | String | Single-valued                 | Filters access permissions by VPC ID. |

### 3.9.4 MapReduce Service (MRS)

IAM provides system-defined identity policies to define common actions supported by cloud services. MRS provides system-defined policies that can be directly used in IAM. You can also create custom policies to supplement system-defined policies for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by MRS, see [Resources](#).

- **Condition Key** contains keys that you can specify in the Condition element of an identity policy statement for MRS.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by MRS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in policy statements for MRS.

**Table 3-195** Actions supported by MRS

| Action                    | Description                             | Access Level | Resource Type (*: required)                    | Condition Key                                          | Alias              |
|---------------------------|-----------------------------------------|--------------|------------------------------------------------|--------------------------------------------------------|--------------------|
| mrs:cluster:createCluster | Grants permissions to create a cluster. | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId | mrs:cluster:create |

| Action                    | Description                                               | Access Level | Resource Type (*: required)                    | Condition Key                                          | Alias              |
|---------------------------|-----------------------------------------------------------|--------------|------------------------------------------------|--------------------------------------------------------|--------------------|
| mrs:cluster:deleteCluster | Grants the permission to delete a cluster.                | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:cluster:delete |
| mrs:cluster:listHosts     | Grants permissions to query nodes in the cluster.         | list         | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:host:list      |
| mrs:cluster:listFiles     | Grants permissions to query the file list in the cluster. | list         | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:file:list      |
| mrs:cluster:createJob     | Grants permissions to execute jobs in the cluster.        | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:job:submit     |
| mrs:cluster:list          | Grants permissions to query the cluster list.             | list         | -                                              | g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId | -                  |
| mrs:cluster:listJobs      | Grants permissions to query the job list of the cluster.  | list         | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:job:list       |
| mrs:cluster:getJob        | Grants permissions to query job details in the cluster.   | read         | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:job:get        |

| Action                        | Description                                                          | Access Level | Resource Type (*: required)                    | Condition Key                                          | Alias                                                    |
|-------------------------------|----------------------------------------------------------------------|--------------|------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------|
| mrs:cluster:getCluster        | Grants permissions to query cluster details.                         | read         | mrs:<region>:<account-id>:cluster:<cluster-id> | -                                                      | mrs:cluster:get                                          |
| mrs:cluster:resizeNodes       | Grants permissions to adjust cluster nodes.                          | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:cluster:resize                                       |
| mrs:cluster:updateClusterName | Grants permissions to rename a cluster.                              | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | -                                                        |
| mrs:cluster:listTags          | Grants permissions to query cluster tags.                            | list         | -                                              | g:EnterpriseProjectId                                  | mrs:tag:list                                             |
| mrs:cluster:updateTags        | Grants permissions to add or delete cluster tags.                    | tagging      | -                                              | g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId | mrs:tag:create<br>mrs:tag:delete<br>mrs:tag:batchOperate |
| mrs:cluster:listClustersByTag | Grants permissions to query the list of clusters with specific tags. | list         | -                                              | g:RequestTag/<tag-key>,g:TagKeys                       | mrs:tag:listResource                                     |
| mrs:cluster:stopJob           | Grants permissions to stop cluster jobs.                             | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId                                  | mrs:job:stop                                             |



| Action                       | Description                                                          | Access Level | Resource Type (*: required)                    | Condition Key         | Alias                               |
|------------------------------|----------------------------------------------------------------------|--------------|------------------------------------------------|-----------------------|-------------------------------------|
| mrs:cluster:deleteJobs       | Grants permissions to delete cluster jobs in batches.                | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | mrs:job:batchDelete                 |
| mrs:cluster:stopSql          | Grants permissions to cancel SQL execution.                          | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | mrs:sql:cancel                      |
| mrs:cluster:createSql        | Grants permissions to submit a SQL statement for execution.          | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | mrs:sql:execute<br>mrs:job:checkSql |
| mrs:cluster:listPolicies     | Grants permissions to obtain all auto scaling policies in a cluster. | list         | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | mrs:cluster:policy                  |
| mrs:cluster:updatePolicies   | Grants permissions to modify auto scaling policies of a cluster.     | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | mrs:cluster:policy                  |
| mrs:cluster:getAgencyMapping | Grants permissions to obtain user agent information.                 | read         | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | -                                   |

| Action                          | Description                                            | Access Level | Resource Type (*: required)                    | Condition Key         | Alias                |
|---------------------------------|--------------------------------------------------------|--------------|------------------------------------------------|-----------------------|----------------------|
| mrs:cluster:updateAgencyMapping | Grants permissions to update user agent information.   | write        | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | mrs:cluster:syncUser |
| mrs:cluster:getSql              | Grants permissions to obtain the SQL execution result. | read         | mrs:<region>:<account-id>:cluster:<cluster-id> | g:EnterpriseProjectId | mrs:sql:get          |

## Resources

A resource type indicates the resources that a policy applies to. If you specify a resource type for any action in [Table 3-196](#), the resource URN must be specified in the policy statements using that action, and the policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the policy applies to all resources. You can also set condition keys in a policy to define resource types.

The following table lists the resource types that you can define in policy statements for MRS.

**Table 3-196** Resource types supported by MRS

| Resource Type | URN                                            |
|---------------|------------------------------------------------|
| cluster       | mrs:<region>:<account-id>:cluster:<cluster-id> |

## Conditions

MRS does not support service-specific condition keys in identity policies.

It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.9.5 Data Warehouse Service (DWS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by dws, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by dws, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for dws.

**Table 3-197** Actions supported by dws

| Action                | Description                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                           | Alias                                                                                                            |
|-----------------------|------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| dws:cluster:list      | Grants permission to query cluster list. | List         | -                           | -                                                                                                                                                                                       | -                                                                                                                |
| dws:cluster:getDetail | Grants permission to get cluster detail. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                      | <ul style="list-style-type: none"> <li>• dws:openAPICluster:getDetail</li> </ul>                                 |
|                       |                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                                                                  |
| dws:cluster:create    | Grants permission to create dws cluster. | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>  | <ul style="list-style-type: none"> <li>• dws:openAPICluster:create</li> <li>• dws:checkCluster:create</li> </ul> |
| dws:cluster:delete    | Grants permission to delete cluster.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                      | <ul style="list-style-type: none"> <li>• dws:openAPICluster:delete</li> </ul>                                    |

| Action               | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                                                                                                                         |
|----------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| dws:cluster:scaleIn  | Grants permission to scale in dws cluster.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dws:cluster:shrink</li> </ul>                                                        |
| dws:cluster:listRing | Grants permission to get ring list.                | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dws:ring:list</li> </ul>                                                             |
| dws:cluster:restore  | Grants permission to restore to the dws cluster.   | Write        | cluster *                   | -                                                                                                                                                                                      | -                                                                                                                             |
|                      |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                                                                               |
| dws:cluster:scaleOut | Grants permission to scale out cluster.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -                                                                                                                             |
| dws:cluster:resize   | Grants permission to scale out cluster and resize. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dws:cluster:scaleOutOpenAPIResize</li> <li>• dws:cluster:checkResizeRetry</li> </ul> |

| Action                           | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                           |
|----------------------------------|--------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| dws:cluster:expandDisk           | Grants permission to expand dws cluster disk.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disk:expand</li> <li>• dws:periodExpandPrecheck:operate</li> </ul> |
| dws:cluster:restart              | Grants permission to restart the cluster.        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:openAPICluster:restart</li> </ul>                                  |
| dws:cluster:resetPassword        | Grants permission to reset the cluster password. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:openAPICluster:resetPassword</li> </ul>                            |
| dws:cluster:listAuditLog         | Grants permission to list audit log.             | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                                               |
| dws:cluster:setMaintenanceWindow | Grants permission to set maintenance window.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                                               |
| dws:cluster:switchover           | Grants permission to cluster switchover.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                                               |

| Action                       | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                        |
|------------------------------|--------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| dws:cluster:cancelReadonly   | Grants permission to cancel read only for dws cluster. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                            |
| dws:cluster:addCN            | Grants permission to add CN node.                      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:module:install         |
| dws:cluster:listCN           | Grants permission to get cluster CN list.              | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                            |
| dws:cluster:deleteCN         | Grants permission to delete CN node.                   | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:module:uninstall       |
| dws:cluster:redistribution   | Grants permission to redistribution.                   | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:redistribution:operate |
| dws:cluster:createDataSource | Grants permission to create MRS connection.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:MRSConnection:create   |

| Action                       | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                        |
|------------------------------|-------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| dws:cluster:updateDataSource | Grants permission to update MRS connection.           | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:MRSConnection:update</li> </ul> |
| dws:cluster:deleteDataSource | Grants permission to delete MRS connection.           | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:MRSConnection:delete</li> </ul> |
| dws:alarm:listConfig         | Grants permission to query alarm config.              | List         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dws:alarmConfig:list</li> </ul>     |
| dws:alarm:listDetail         | Grants permission to query alarm details.             | List         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dws:alarmDetail:list</li> </ul>     |
| dws:alarm:listStatistics     | Grants permission to query alarm statics.             | List         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dws:alarmStatistic:list</li> </ul>  |
| dws:alarm:createSubscription | Grants permission to create alarm subscription.       | Write        | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dws:alarmSub:create</li> </ul>      |
| dws:alarm:listSubscription   | Grants permission to query alarm subscription.        | List         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dws:alarmSub:list</li> </ul>        |
| dws:alarm:updateSubscription | Grants permission to update query alarm subscription. | Write        | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dws:alarmSub:update</li> </ul>      |



| Action                       | Description                                           | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                 |
|------------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------|
| dws:alarm:deleteSubscription | Grants permission to delete query alarm subscription. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>dws:alarmSub:delete</li> </ul> |
| dws:alarm:report             | Grants permission to report alarm.                    | Write        | -                           | -             | -                                                                     |
| dws:event:list               | Grants permission to query event lists.               | List         | -                           | -             | -                                                                     |
| dws:event:listSpec           | Grants permission to query event configuration.       | List         | -                           | -             | <ul style="list-style-type: none"> <li>dws:eventSpec:list</li> </ul>  |
| dws:event:listSubscription   | Grants permission to query event subscription.        | Read         | -                           | -             | <ul style="list-style-type: none"> <li>dws:eventSub:list</li> </ul>   |
| dws:event:createSpec         | Grants permission to create event configuration.      | Write        | -                           | -             | -                                                                     |
| dws:event:deleteSpec         | Grants permission to delete event configuration.      | Write        | -                           | -             | -                                                                     |
| dws:event:createSubscription | Grants permission to create event subscription.       | Write        | -                           | -             | <ul style="list-style-type: none"> <li>dws:eventSub:create</li> </ul> |
| dws:event:updateSubscription | Grants permission to update event subscription.       | Write        | -                           | -             | <ul style="list-style-type: none"> <li>dws:eventSub:update</li> </ul> |

| Action                       | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                 |
|------------------------------|---------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| dws:event:deleteSubscription | Grants permission to delete event subscription.   | Write        | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>dws:eventSub:delete</li> </ul> |
| dws:event:report             | Grants permission to report event.                | Write        | -                           | -                                                                                                                                              | -                                                                     |
| dws:cluster:createConnection | Grants permission to create dws connection.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dws:dns:create</li> </ul>      |
| dws:cluster:deleteConnection | Grants permission to delete dws connection.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dws:dns:release</li> </ul>     |
| dws:cluster:updateConnection | Grants permission to update dws connection.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dws:dns:edit</li> </ul>        |
| dws:cluster:bindEIP          | Grants permission to public network IP binding.   | Write        | cluster *                   | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dws:eip:operate</li> </ul>     |
| dws:cluster:unbindEIP        | Grants permission to public network IP unbinding. | Write        | cluster *                   | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dws:eip:operate</li> </ul>     |

| Action                             | Description                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| dws:cluster:listELB                | Grants permission to list elb.                            | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:elb:list</li> </ul>                                                                              |
| dws:cluster:bindELB                | Grants permission to bind elb.                            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:elb:bind</li> </ul>                                                                              |
| dws:cluster:unbindELB              | Grants permission to unbind elb.                          | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:elb:unbind</li> </ul>                                                                            |
| dws:cluster:createSnapshotPolicy   | Grants permission to set up an automatic snapshot policy. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:cluster:setAutomatedSnapshot</li> </ul>                                                          |
| dws:cluster:listSnapshotStatistics | Grants permission to dws cluster snapshot statistics.     | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                                                                             |
| dws:cluster:listSnapshot           | Grants permission to view cluster snapshot list.          | List         | cluster                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:openAPISnapshot:list</li> <li>• dws:clusterSnapshot:list</li> <li>• dws:snapshot:list</li> </ul> |

| Action                           | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                                         |
|----------------------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| dws:cluster:getSnapshotDetail    | Grants permission to view cluster snapshot detail. | List         | cluster                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:openAPISnapshot:detail</li> </ul>                                |
| dws:cluster:createSnapshot       | Grants permission to create snapshot.              | Write        | cluster*                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:openAPISnapshot:create</li> <li>• dws:snapshot:create</li> </ul> |
| dws:cluster:deleteSnapshotPolicy | Grants permission to delete snapshot policy.       | Write        | cluster*                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:backupPolicy:delete</li> </ul>                                   |
| dws:cluster:listSnapshotPolicy   | Grants permission to query snapshot policy.        | List         | cluster*                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                                             |
| dws:cluster:copySnapshot         | Grants permission to copy snapshot.                | Write        | cluster*                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:snapshot:copy</li> </ul>                                         |
| dws:cluster:deleteSnapshot       | Grants permission to delete snapshots.             | Write        | cluster*                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:openAPISnapshot:delete</li> <li>• dws:snapshot:delete</li> </ul> |

| Action                                 | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                 |
|----------------------------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| dws:cluster:restoreSnapshot            | Grants permission to restore snapshots.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:openAPISnapshot:restore</li> </ul>       |
| dws:cluster:deleteDisasterRecovery     | Grants permission to delete disaster recovery.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:delete</li> </ul>       |
| dws:cluster:createDisasterRecovery     | Grants permission to create disaster recovery.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:create</li> </ul>       |
| dws:cluster:startDisasterRecovery      | Grants permission to start disaster-recovery.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:otherOperate</li> </ul> |
| dws:cluster:pauseDisasterRecovery      | Grants permission to pause disaster-recovery.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:otherOperate</li> </ul> |
| dws:cluster:switchoverDisasterRecovery | Grants permission to switchover disaster-recovery. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:otherOperate</li> </ul> |

| Action                             | Description                                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                                                                                 |
|------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| dws:cluster:switchFailoverDisaster | Grants permission to other switch failover disaster-recovery.                                                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:otherOperate</li> </ul> |
| dws:cluster:restoreDisaster        | Grants permission to restore disaster-recovery.                                                              | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:otherOperate</li> </ul> |
| dws:cluster:getDisasterRecovery    | Grants permission to get disaster-recovery detail.                                                           | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:get</li> </ul>          |
| dws::listTagsForProject            | Grants permission to query the list of tags corresponding to a single resource(using in console and shared). | List         | -                           | -                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• dws:openAPITag:list</li> </ul>               |
| dws::listTagsForResource           | Grants permission to query the cluster tag list(using in console and shared).                                | List         | cluster *                   | -                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• dws:openAPITag:getResourceTag</li> </ul>     |
|                                    |                                                                                                              |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                                       |
| dws::tagResource                   | Grants permission to add tag.                                                                                | Tagging      | cluster *                   | -                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• dws:openAPITag:add</li> </ul>                |

| Action                               | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                                                                     |
|--------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|                                      |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                           |
| dws::unTagResource                   | Grants permission to delete tag.                                 | Tagging      | cluster *                   | -                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• dws:openAPItag:delete</li> </ul> |
|                                      |                                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                           |
| dws:monitor:listHostDisk             | Grants permission to list host disk for dms monitoring.          | List         | -                           | -                                                                                                                                                                                      | -                                                                         |
| dws:monitor:listHostNet              | Grants permission to list host network for dms monitoring.       | List         | -                           | -                                                                                                                                                                                      | -                                                                         |
| dws:monitor:listMonitorIndicatorData | Grants permission to list monitor history for dms monitoring.    | List         | -                           | -                                                                                                                                                                                      | -                                                                         |
| dws:monitor:listMonitorIndicators    | Grants permission to list monitor indicators for dms monitoring. | List         | -                           | -                                                                                                                                                                                      | -                                                                         |

| Action                     | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                               |
|----------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| dws:cluster:listConfig     | Grants permission to list cluster configuration.     | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                   |
| dws:service:listSpec       | Grants permission to list service spec.              | List         | -                           | -                                                                                                                                                  | <ul style="list-style-type: none"> <li>• dws:specProduct:list</li> </ul>            |
| dws:cluster:listDataSource | Grants permission to list dataSource.                | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:MRSSource:list</li> </ul>              |
| dws:service:listJobDetail  | Grants permission to list job detail.                | List         | -                           | -                                                                                                                                                  | -                                                                                   |
| dws:service:listStatistics | Grants permission to list resource statics.          | List         | -                           | -                                                                                                                                                  | -                                                                                   |
| dws:service:listQuotas     | Grants permission to get user quotas.                | List         | -                           | -                                                                                                                                                  | -                                                                                   |
| dws:cluster:updateConfig   | Grants permission to update cluster configuration.   | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:cluster:setSecuritySettings</li> </ul> |
| dws:service:listAZ         | Grants permission to list service availability zone. | List         | -                           | -                                                                                                                                                  | -                                                                                   |



| Action                        | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                    | Alias                                                                                         |
|-------------------------------|--------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| dws:service:listDssPools      | Grants permission to list dec storage pool.      | List         | -                           | -                                                                                                                                                                                | -                                                                                             |
| dws:service:listEps           | Grants permission to list eps.                   | List         | -                           | -                                                                                                                                                                                | -                                                                                             |
| dws:service:authorize         | Grants permission to authorize.                  | Write        | -                           | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>dws:authorize:operate</li> </ul>                       |
| dws:service:checkAuthorize    | Grants permission to check authorize.            | Read         | -                           | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>dws:checkAuthorize:operate</li> </ul>                  |
| dws::updateTag                | Grants permission to update tag.                 | Tagging      | cluster *                   | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>dws:tag:edit</li> <li>dws:openAPITag:update</li> </ul> |
|                               |                                                  |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                                               |
| dws:cluster:getSnapshotPolicy | Grants permission to get snapshot policy detail. | Read         | cluster *                   | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                   | <ul style="list-style-type: none"> <li>dws:backupPolicy:list</li> </ul>                       |
| dws:cluster:bindOrUnbindELB   | Grants permission to bind or unbind elb.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                   | <ul style="list-style-type: none"> <li>dws:elb:bind</li> </ul>                                |

| Action                      | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                      |
|-----------------------------|-------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| dws:cluster:bindOrUnbindEIP | Grants permission to bind or unbind eip.        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:eip:operate          |
| dws:cluster:deleteNode      | Grants permission to delete node.               | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:clusterNodes:operate |
| dws:cluster:listConnection  | Grants permission to query dws connection list. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:dns:list             |
| dws:cluster:checkConnection | Grants permission to check dws connection.      | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                          |
| dws:cluster:listDN          | Grants permission to get cluster DN list.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                          |
| dws:cluster:listBucket      | Grants permission to get bucket list.           | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                          |

| Action                           | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                                                                               |
|----------------------------------|---------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| dws:cluster:listScaleInNode      | Grants permission to get scale in node list.      | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -                                                                                   |
| dws:cluster:listFlavorForResize  | Grants permission to get flavor for resize list.  | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -                                                                                   |
| dws:cluster:listFlavorForRestore | Grants permission to get flavor for restore list. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -                                                                                   |
| dws::countResourceByTag          | Grants permission to query cluster by tag.        | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -                                                                                   |
| dws:cluster:updateSnapshotPolicy | Grants permission to update snapshot policy.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• dws:backupPolicyDetail:update</li> </ul>   |
| dws::listResourceByTag           | Grants permission to query cluster list by tag.   | List         | cluster *                   | -                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>• dws:openAPITag:getResourceByTag</li> </ul> |
|                                  |                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                                     |

| Action                                    | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                 |
|-------------------------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| dws:cluster:assessRisk                    | Grants permission to assess risk for resize.            | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                     |
| dws:cluster:checkRestoreTable             | Grants permission to check restore table.               | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:tableRestoreCheck:operate</li> </ul>     |
| dws:cluster:checkSupportFineGrainedBackup | Grants permission to check support fine grained backup. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:checkSupport:operate</li> </ul>          |
| dws:cluster:configureNetwork              | Grants permission to configure cluster network.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                     |
| dws:cluster:expandWithExistedNodes        | Grants permission to expand cluster from free node.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:expandWithExistedNodes:update</li> </ul> |
| dws:cluster:getAntiAffinity               | Grants permission to get anti affinity.                 | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                     |

| Action                             | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getCnCount             | Grants permission to query cluster CN count.                  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getCredential          | Grants permission to get cluster JDBC connection credentials. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getDiskExpandScope     | Grants permission to get disk expand scope.                   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getEncryptInfo         | Grants permission to get cluster encrypt info.                | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listHistoryConfig      | Grants permission to list history config record.              | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getHistoryConfigDetail | Grants permission to get history config record detail.        | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                             | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                         |
|------------------------------------|-------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| dws:cluster:getInstanceDetail      | Grants permission to get instance detail.       | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:getProcessTopo         | Grants permission to get cluster process topo.  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:processTopo:list        |
| dws:cluster:getRedistribution      | Grants permission to query redistribution info. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:redistributionInfo:list |
| dws:cluster:getRestoreDatabase     | Grants permission to get restore database.      | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:getRoachConfig         | Grants permission to get roach config.          | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:roachConfig:get         |
| dws:cluster:getSnapshotEncryptInfo | Grants permission to get snapshot encrypt info. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:clusterEncryptInfo:list |

| Action                         | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias              |
|--------------------------------|---------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| dws:cluster:getSnapshotStorage | Grants permission to query snapshot storage info. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                  |
| dws:cluster:getTaskDetail      | Grants permission to query cluster task detail.   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                  |
| dws:cluster:getVolumeInfo      | Grants permission to query volume info.           | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                  |
| dws:cluster:listNode           | Grants permission to get cluster node list.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                  |
| dws:cluster:listSchema         | Grants permission to get schema list.             | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:schemas:list |
| dws:cluster:listTable          | Grants permission to get table list.              | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:tables:list  |

| Action                            | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                             |
|-----------------------------------|-----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| dws:cluster:listDatabase          | Grants permission to get user database list.        | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:userDatabase:list</li> </ul>         |
| dws:cluster:recoverRedistribution | Grants permission to recover redistribution.        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:redistribution:recover</li> </ul>    |
| dws:cluster:resizeFlavor          | Grants permission to resize flavor.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:specResize:operate</li> </ul>        |
| dws:cluster:resizeRetry           | Grants permission to execute retry for resize.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:cluster:submitResizeRetry</li> </ul> |
| dws:cluster:restoreTable          | Grants permission to restore table.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:tableRestore:operate</li> </ul>      |
| dws:cluster:retryELBSwitch        | Grants permission to retry ELB switch servers task. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                 |



| Action                              | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                          |
|-------------------------------------|-----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| dws:cluster:listRingForScaleIn      | Grants permission to list ring for scale in.        | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| dws:cluster:saveDescriptionInfo     | Grants permission to save cluster description info. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| dws:cluster:stopSnapshot            | Grants permission to stop snapshot.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:snapshot:stop            |
| dws:cluster:suspendRedistribution   | Grants permission to suspend redistribution.        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:redistribution:suspend   |
| dws:cluster:updateInstanceAliasName | Grants permission to update instance alias name.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:instanceAliasName:update |
| dws:cluster:updateRoachConfig       | Grants permission to update roach config.           | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:roachConfig:update       |

| Action                                   | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                 |
|------------------------------------------|-------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| dws:cluster:updateScheduleConfig         | Grants permission to update schedule config.          | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:roachConfig:update</li> </ul>            |
| dws:service:getClusterSum                | Grants permission to query cluster count.             | Read         | -                           | -                                                                                                                                                  | -                                                                                     |
| dws:service:getResourceStatistics        | Grants permission to query resource statistics.       | Read         | -                           | -                                                                                                                                                  | -                                                                                     |
| dws:service:getStorageStatistics         | Grants permission to query storage statistics.        | Read         | -                           | -                                                                                                                                                  | -                                                                                     |
| dws:cluster:listDisasterRecovery         | Grants permission to get disaster-recovery list.      | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:get</li> </ul>          |
| dws:cluster:checkDisasterRecoveryName    | Grants permission to check disaster-recovery name.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:get</li> </ul>          |
| dws:cluster:updateDisasterRecoveryConfig | Grants permission to update disaster-recovery config. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:otherOperate</li> </ul> |

| Action                              | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                           |
|-------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| dws:cluster:addOperationalTask      | Grants permission to add schedule task.                          | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:operationalTask:operate</li> </ul> |
| dws:cluster:bindManagelp            | Grants permission to bind the management plane IP address.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:bindManagelp:operate</li> </ul>    |
| dws:cluster:checkAccessLts          | Grants permission to check whether the LTS service is normal.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:ltsAccess:get</li> </ul>           |
| dws:cluster:checkLogicalClusterData | Grants permission to check whether the cluster has service data. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:logicalCluster:get</li> </ul>      |
| dws:cluster:closeAccessLts          | Grants permission to close cloud service log.                    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:ltsAccess:operate</li> </ul>       |
| dws:cluster:createLogicalCluster    | Grants permission to create logical cluster.                     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:logicalCluster:operate</li> </ul>  |

| Action                             | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:createApplicationForDM | Grants permission to add Job Task for data migration.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:createClusterForDM     | Grants permission to create cluster for data migration.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:createConnectionForDM  | Grants permission to create connection for data migration. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:createMappingForDM     | Grants permission to create mapping for data migration.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deleteApplicationForDM | Grants permission to delete job task for data migration.   | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deleteClusterForDM     | Grants permission to delete cluster for data migration.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                 | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:deleteConnectionForDM      | Grants permission to delete connection for data migration.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deleteMappingForDM         | Grants permission to delete mapping for data migration.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:dialsConnectionForDM       | Grants permission to detect connection for data migration.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getApplicationForDM        | Grants permission to get job task detail for data migration.  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listApplicationConfigForDM | Grants permission to list job task config for data migration. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listApplicationForDM       | Grants permission to list job task for data migration.        | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                     | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getClusterForDM                | Grants permission to get cluster detail for data migration.   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listClusterForDM               | Grants permission to get cluster for data migration.          | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listConfigurationTemplateForDM | Grants permission to list config template for data migration. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getConnectionForDM             | Grants permission to get connection for data migration.       | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listConnectionForDM            | Grants permission to list connection for data migration.      | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listDependApplicationForDM     | Grants permission to list depend job task for data migration. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                            | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getMappingForDM       | Grants permission to get mapping detail for data migration. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listMappingForDM      | Grants permission to list mapping for data migration.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listProductForDM      | Grants permission to list product for data migration.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updateConnectionForDM | Grants permission to update connection for data migration.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updateMappingForDM    | Grants permission to update mapping for data migration.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:startApplicationForDM | Grants permission to start job task for data migration.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                      | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                  |
|---------------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| dws:cluster:stopApplicationForDM            | Grants permission to stop job task for data migration.                               | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                                      |
| dws:cluster:deleteCrossRegionSnapshotPolicy | Grants permission to delete cross region snapshot policy.                            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:crossRegionBackupConfig:delete</li> </ul> |
| dws:cluster:deleteLogicalCluster            | Grants permission to delete logical cluster.                                         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:logicalCluster:operate</li> </ul>         |
| dws:cluster:deleteOperationalTask           | Grants permission to delete operational task.                                        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:operationalTask:operate</li> </ul>        |
| dws:cluster:operateDisasterRecovery         | Grants permission to operate disaster-recovery, such as start, stop, and switchover. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:otherOperate</li> </ul>  |
| dws:cluster:updateLogicalCluster            | Grants permission to update logical cluster.                                         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:logicalCluster:operate</li> </ul>         |



| Action                                       | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                      |
|----------------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| dws:cluster:listAllCrossRegionSnapshotConfig | Grants permission to list all cross region snapshot config. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                          |
| dws:cluster:getDisasterRecoveryProject       | Grants permission to get disaster-recovery project.         | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:disasterRecovery:get |
| dws:cluster:getDisasterRecoveryRegion        | Grants permission to get disaster-recovery region.          | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:disasterRecovery:get |
| dws:cluster:getLastOperationalTask           | Grants permission to get last operational task.             | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:operationalTask:get  |
| dws:cluster:getLogicalClusterRings           | Grants permission to get logical cluster rings.             | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:logicalCluster:get   |
| dws:cluster:getLogicalClusterVolume          | Grants permission to get logical cluster volume.            | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:logicalCluster:get   |

| Action                                            | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                        |
|---------------------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| dws:cluster:getOperationalTaskConfig              | Grants permission to get operational task config.                 | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:operationalTask:get    |
| dws:cluster:getOperationalTaskDetail              | Grants permission to get operational task detail.                 | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:operationalTask:get    |
| dws:cluster:getOperationalTaskStatus              | Grants permission to get operational task status.                 | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:operationalTask:get    |
| dws:cluster:listSnapshotRegion                    | Grants permission to list snapshot region.                        | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                            |
| dws:cluster:getTargetAllCrossRegionSnapshotConfig | Grants permission to get target all cross region snapshot config. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                            |
| dws:cluster:initLogicalClusterSwitch              | Grants permission to init logical cluster switch.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:logicalCluster:operate |

| Action                             | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                         |
|------------------------------------|-------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| dws:cluster:listAccessLts          | Grants permission to list access Lts.           | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:listLogicalCluster     | Grants permission to list logical cluster.      | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:logicalCluster:get      |
| dws:cluster:listLogicalClusterTask | Grants permission to list logical cluster task. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:logicalCluster:get      |
| dws:cluster:listOperationalTask    | Grants permission to list operational task.     | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:operationalTask:get     |
| dws:cluster:openAccessLts          | Grants permission to open cloud service log.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:ltsAccess:operate       |
| dws:cluster:pauseOperationalTask   | Grants permission to pause operational task.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:operationalTask:operate |

| Action                                   | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                                  |
|------------------------------------------|--------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| dws:cluster:getDisasterRecoveryDetail    | Grants permission to get disaster-recovery detail.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:disasterRecovery:get</li> </ul>           |
| dws:cluster:refreshOperationalTask       | Grants permission to refresh operational task.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:operationalTask:get</li> </ul>            |
| dws:cluster:restartLogicalCluster        | Grants permission to restart logical cluster.          | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:logicalCluster:operate</li> </ul>         |
| dws:cluster:resumeOperationalTask        | Grants permission to resume operational task.          | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:operationalTask:operate</li> </ul>        |
| dws:cluster:setCrossRegionSnapshotPolicy | Grants permission to set cross region snapshot policy. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:crossRegionBackupConfig:update</li> </ul> |
| dws:cluster:startOperationalTask         | Grants permission to start operational task.           | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:operationalTask:operate</li> </ul>        |

| Action                                       | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                         |
|----------------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| dws:cluster:stopOperationalTask              | Grants permission to stop operational task.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:operationalTask:operate |
| dws:cluster:switchLogicalCluster             | Grants permission to switch logical cluster.                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:logicalCluster:operate  |
| dws:cluster:syncCrossRegionBackupClusterInfo | Grants permission to sync cross region backup cluster info. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:syncCrossRegionBackupConfig      | Grants permission to sync cross region backup config.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:syncCrossRegionBackupInfo        | Grants permission to sync cross region backup info.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:syncLogicalCluster               | Grants permission to sync logical cluster.                  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:logicalCluster:get      |

| Action                                  | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                           |
|-----------------------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| dws:cluster:updateOperationalTaskConfig | Grants permission to update operational task config.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:operationalTask:get</li> </ul>     |
| dws:cluster:updateOperationalTask       | Grants permission to update operational task.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:operationalTask:operate</li> </ul> |
| dws:cluster:addPlanForWLM               | Grants permission to add plan for workload manger.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:addPlanStageForWLM          | Grants permission to add plan stage for workload manger. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:addQueueForWLM              | Grants permission to add queue for workload manger.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:addQueueUserForWLM          | Grants permission to add queue user for workload manger. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |

| Action                            | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                           |
|-----------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| dws:cluster:deletePlanForWLM      | Grants permission to delete plan for workload manger.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:deletePlanStageForWLM | Grants permission to delete plan stage for workload manger. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:deleteQueueForWLM     | Grants permission to delete queue for workload manger.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:deleteQueueUserForWLM | Grants permission to delete queue user for workload manger. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:exportPlanForWLM      | Grants permission to export plan for workload manger.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:getPlanDetailForWLM   | Grants permission to get plan detail for workload manger.   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |

| Action                           | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                       |
|----------------------------------|------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| dws:cluster:getPlanLogForWLM     | Grants permission to get plan log for workload manger.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul> |
| dws:cluster:getPlanQueueForWLM   | Grants permission to get plan queue for workload manger.   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul> |
| dws:cluster:getPlanStageForWLM   | Grants permission to get plan stage for workload manger.   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul> |
| dws:cluster:listQueueForWLM      | Grants permission to list queue for workload manger.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul> |
| dws:cluster:getQueueDetailForWLM | Grants permission to get queue detail for workload manger. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul> |
| dws:cluster:getQueueRuleForWLM   | Grants permission to get queue rule for workload manger.   | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul> |



| Action                             | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                           |
|------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| dws:cluster:importPlanForWLM       | Grants permission to import plan for workload manger.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:listPlanQueueForWLM    | Grants permission to list plan queue for workload manger.     | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:listPlanForWLM         | Grants permission to list plan for workload manger.           | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:listQueueUserForWLM    | Grants permission to list queue user for workload manger.     | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:listUserForWLM         | Grants permission to list user for workload manger.           | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:getClusterDBInfoForWLM | Grants permission to get cluster DB info for workload manger. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |

| Action                                 | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                           |
|----------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| dws:cluster:listClusterPlanForWLM      | Grants permission to list cluster plan for workload manger.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:getClusterSchemaInfoForWLM | Grants permission to get cluster schema info for workload manger. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:getClusterVersionForWLM    | Grants permission to get cluster version for workload manger.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:getFunctionStatusForWLM    | Grants permission to get function status for workload manger.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:get</li> </ul>     |
| dws:cluster:setFunctionStatusForWLM    | Grants permission to set function status for workload manger.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |
| dws:cluster:startPlanForWLM            | Grants permission to start plan for workload manger.              | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:workLoadManager:operate</li> </ul> |

| Action                                | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                         |
|---------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| dws:cluster:stopPlanForWLM            | Grants permission to stop plan for workload manger.             | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:workLoadManager:operate |
| dws:cluster:switchPlanStageForWLM     | Grants permission to switch plan stage for workload manger.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:workLoadManager:operate |
| dws:cluster:updatePlanStageForWLM     | Grants permission to update plan stage for workload manger.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:workLoadManager:operate |
| dws:cluster:updateQueueBaseForWLM     | Grants permission to update queue base for workload manger.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:workLoadManager:operate |
| dws:cluster:updateQueueResourceForWLM | Grants permission to update queue resource for workload manger. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:workLoadManager:operate |
| dws:cluster:updateQueueRuleForWLM     | Grants permission to update queue rule for workload manger.     | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:workLoadManager:operate |

| Action                                | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                         |
|---------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| dws:cluster:updateSchemaLimitForWLM   | Grants permission to update schema limit for workload manager.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:workLoadManager:operate |
| dws:cluster:getMonitorConfigForDMS    | Grants permission to get monitor config for dms monitoring.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:monitor:listClusterOverview       | Grants permission to list cluster overview for dms monitoring.  | List         | -                           | -                                                                                                                                                  | -                             |
| dws:cluster:listClusterInstanceForDMS | Grants permission to list cluster instance for dms monitoring.  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:getDDLExamineDetailForDMS | Grants permission to get ddl examine detail for dms monitoring. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |
| dws:cluster:getClusterDnStreamForDMS  | Grants permission to get cluster DN stream for dms monitoring.  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                             |

| Action                                 | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:listClusterAlarmRuleForDMS | Grants permission to list cluster alarm rule for dms monitoring. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getClusterInstanceForDMS   | Grants permission to get cluster instance for dms monitoring.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getHostNetMetricsForDMS    | Grants permission to get host net metrics for dms monitoring.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:getHistoryMetrics          | Grants permission to get history metrics for dms monitoring.     | Read         | -                           | -                                                                                                                                                  | -     |
| dws:cluster:getMonitoringInfoForDMS    | Grants permission to get monitoring info for dms monitoring.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listAlarmRuleForDMS        | Grants permission to list alarm rule for dms monitoring.         | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                     | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:updateCollectionItemForDMS     | Grants permission to update collection item for dms monitoring.      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:doDDLExamineActionForDMS       | Grants permission to do ddl examine action for dms monitoring.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:downloadDDLExamineDetailForDMS | Grants permission to download ddl examine detail for dms monitoring. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listInstanceDiskIOForDMS       | Grants permission to list instance disk io for dms monitoring.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:resetCollectionItemForDMS      | Grants permission to reset collection item for dms monitoring.       | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getQueryRangeForDMS            | Grants permission to get query range for dms monitoring.             | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                     | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:monitor:getAlarmConfig                 | Grants permission to get alarm config for dms monitoring.           | Read         | -                           | -                                                                                                                                                  | -     |
| dws:cluster:switchoverCollectionItemForDMS | Grants permission to switchover collection item for dms monitoring. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:getOSMetrics                   | Grants permission to get OS metrics for dms monitoring.             | Read         | -                           | -                                                                                                                                                  | -     |
| dws:cluster:listPerfDashboardForDMS        | Grants permission to list perf dashboard for dms monitoring.        | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:disableCollectionItemForDMS    | Grants permission to disable collection item for dms monitoring.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:getAggregationOSMetrics        | Grants permission to get aggregation OS metrics for dms monitoring. | Read         | -                           | -                                                                                                                                                  | -     |

| Action                                       | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|----------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:terminateSessionForDMS           | Grants permission to terminate session for dms monitoring.             | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getPerfDashboardDetailForDMS     | Grants permission to get perf dashboard detail for dms monitoring.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:createAlarmRule                  | Grants permission to create alarm rule for dms monitoring.             | Write        | -                           | -                                                                                                                                                  | -     |
| dws:cluster:enableCollectionItemForDMS       | Grants permission to enable collection item for dms monitoring.        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listInstanceNetworkMetricsForDMS | Grants permission to list instance network metrics for dms monitoring. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:createPerfDashboardForDMS        | Grants permission to create perf dashboard for dms monitoring.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |



| Action                                         | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getMonitorMetricsForDMS            | Grants permission to get monitor metrics for dms monitoring.              | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:createSQLProbeForDMS               | Grants permission to create SQL probe for dms monitoring.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listInstanceIOStatusForDMS         | Grants permission to list instance IO status for dms monitoring.          | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getMonitorMetricsByDimensionForDMS | Grants permission to get monitor metrics by dimension for dms monitoring. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updateStorageConfigForDMS          | Grants permission to update storage config for dms monitoring.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:updateAlarmRule                    | Grants permission to update alarm rule for dms monitoring.                | Write        | -                           | -                                                                                                                                                  | -     |

| Action                                          | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getInstanceIOAggResultForDMS        | Grants permission to get instance IO agg result for dms monitoring.       | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updatePerfDashboardForDMS           | Grants permission to update perf dashboard for dms monitoring.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getMonitorHistoryMetricsCost        | Grants permission to get monitor history metrics for dms monitoring.      | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:deleteAlarmRule                     | Grants permission to delete alarm rule for dms monitoring.                | Write        | -                           | -                                                                                                                                                  | -     |
| dws:cluster:updateSQLProbeForDMS                | Grants permission to update SQL probe for dms monitoring.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:startMonitorMetricsCollectionForDMS | Grants permission to start monitor metrics collection for dms monitoring. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                         | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:listInstanceStorageForDMS          | Grants permission to list instance storage for dms monitoring.           | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deletePerfDashboardForDMS          | Grants permission to delete perf dashboard for dms monitoring.           | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getMonitorMetricsDetailForDMS      | Grants permission to get monitor metrics detail for dms monitoring.      | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deleteSQLProbeForDMS               | Grants permission to delete SQL probe for dms monitoring.                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:stopAlarmRule                      | Grants permission to stop alarm rule for dms monitoring.                 | Write        | -                           | -                                                                                                                                                  | -     |
| dws:cluster:stopMonitorMetricsCollectionForDMS | Grants permission to stop monitor metrics collection for dms monitoring. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                  | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:listExceptionTableForDMS    | Grants permission to list exception table for dms monitoring.     | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getInstanceStorageAggForDMS | Grants permission to get instance storage agg for dms monitoring. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getWDRSnapshotForDMS        | Grants permission to get WDR snapshot for dms monitoring.         | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getPerfMetricsDataForDMS    | Grants permission to get perf metrics data for dms monitoring.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listQueryForDMS             | Grants permission to list query for dms monitoring.               | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getInstanceIOMetricsForDMS  | Grants permission to get instance IO metrics for dms monitoring.  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                           | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getSQLProbeDetailForDMS              | Grants permission to get SQL probe detail for dms monitoring.              | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:switchoverMonitorMetricsStatusForDMS | Grants permission to switchover monitor metrics status for dms monitoring. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:startAlarmRule                       | Grants permission to start alarm rule for dms monitoring.                  | Write        | -                           | -                                                                                                                                                  | -     |
| dws:monitor:getClusterStatus                     | Grants permission to get cluster status for dms monitoring.                | Read         | -                           | -                                                                                                                                                  | -     |
| dws:cluster:getPerfMetricsDetailForDMS           | Grants permission to get perf metrics detail for dms monitoring.           | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listSlowInstanceForDMS               | Grants permission to list slow instance for dms monitoring.                | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                    | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getDDLExamineConfigForDMS     | Grants permission to get ddl examine config for dms monitoring.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getMonitoringViewStatusForDMS | Grants permission to get monitoring view status for dms monitoring. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:enableAlarm                   | Grants permission to enable alarm for dms monitoring.               | Write        | -                           | -                                                                                                                                                  | -     |
| dws:cluster:createWDRSnapshotForDMS       | Grants permission to create WDR snapshot for dms monitoring.        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listExecuteStatusForDMS       | Grants permission to list execute status for dms monitoring.        | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getSlowInstanceDetailForDMS   | Grants permission to get slow instance detail for dms monitoring.   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                              | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:enableSQLProbeForDMS    | Grants permission to enable SQL probe for dms monitoring.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getWDRConfigForDMS      | Grants permission to get WDR config for dms monitoring.      | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:disableAlarm            | Grants permission to disable alarm for dms monitoring.       | Write        | -                           | -                                                                                                                                                  | -     |
| dws:cluster:getMonitoringViewForDMS | Grants permission to get monitoring view for dms monitoring. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getDatabaseUsageForDMS  | Grants permission to get database usage for dms monitoring.  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listSQLProbeForDMS      | Grants permission to list SQL probe for dms monitoring.      | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:monitor:getAlarmMetrics           | Grants permission to get alarm metrics for dms monitoring.     | Read         | -                           | -                                                                                                                                                  | -     |
| dws:monitor:listMetricStatus          | Grants permission to list metrics status for dms monitoring.   | List         | -                           | -                                                                                                                                                  | -     |
| dws:cluster:listSessionStatusForDMS   | Grants permission to list session status for dms monitoring.   | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:downloadPerfHistoryForDMS | Grants permission to download perf history for dms monitoring. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:addPerfItemForDMS         | Grants permission to add perf item for dms monitoring.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listClusterSessionForDMS  | Grants permission to list cluster session for dms monitoring.  | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |



| Action                              | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getSQLDiagnosticsForDMS | Grants permission to get SQL diagnostics for dms monitoring. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updateWDRSnapshotForDMS | Grants permission to update WDR snapshot for dms monitoring. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:clearAlarm              | Grants permission to clear alarm for dms monitoring.         | Write        | -                           | -                                                                                                                                                  | -     |
| dws:cluster:executeSQLProbeForDMS   | Grants permission to execute SQL probe for dms monitoring.   | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listQueryStatusForDMS   | Grants permission to list query status for dms monitoring.   | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getWDRReportForDMS      | Grants permission to get WDR report for dms monitoring.      | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                              | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:listWLMQueueForDMS      | Grants permission to list workload manager queue for dms monitoring. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updatePerfItemForDMS    | Grants permission to update perf item for dms monitoring.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getQueryCostForDMS      | Grants permission to get query cost for dms monitoring.              | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:createWDRReportForDMS   | Grants permission to create WDR report for dms monitoring.           | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:downloadWDRReportForDMS | Grants permission to download WDR report for dms monitoring.         | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listDatabaseForDMS      | Grants permission to list database for dms monitoring.               | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                               | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:listUserWLMQueueForDMS   | Grants permission to list user workload manager queue for dms monitoring. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deletePerfItemForDMS     | Grants permission to delete perf item for dms monitoring.                 | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:monitor:getExceptionAlarmRule    | Grants permission to get exception alarm rule for dms monitoring.         | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getWDRHostForDMS         | Grants permission to get WDR host for dms monitoring.                     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getHistoryPerfDataForDMS | Grants permission to get history perf data for dms monitoring.            | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deleteWDRReportForDMS    | Grants permission to delete WDR report for dms monitoring.                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                     | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getPerfDetailByDimensionForDMS | Grants permission to get perf detail by dimension for dms monitoring. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:downloadPerfHistoryByIdForDMS  | Grants permission to download perf history by id for dms monitoring.  | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listWaitingWLMForDMS           | Grants permission to list waiting WLM for dms monitoring.             | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getQueryPropertyForDMS         | Grants permission to get query property for dms monitoring.           | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listBucketForDMS               | Grants permission to list bucket for dms monitoring.                  | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getHistoryQueryPropertyForDMS  | Grants permission to get history query property for dms monitoring.   | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                             | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:listExceptionWLMForDMS | Grants permission to list exception WLM for dms monitoring. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:terminateQueryForDMS   | Grants permission to terminate query for dms monitoring.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updateTaskForDMS       | Grants permission to update task for dms monitoring.        | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:retryTaskForDMS        | Grants permission to retry task for dms monitoring.         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listTaskForDMS         | Grants permission to list task for dms monitoring.          | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:syncIamUser            | Grants permission to sync IAM user.                         | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                              | Description                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------|-------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:listDatabaseUser        | Grants permission to list database user.        | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getDatabaseUser         | Grants permission to get database user.         | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updateDatabaseUserInfo  | Grants permission to update database user info. | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:updateDatabaseAuthority | Grants permission to update database authority. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getDatabaseAuthority    | Grants permission to get database authority.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getDisasterProgress     | Grants permission to get disaster progress.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                  | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------------------------|-------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getDatabaseOmUserStatus     | Grants permission to get database om user status.     | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:executeDatabaseOmUserAction | Grants permission to execute database om user action. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getClusterInstancesInfo     | Grants permission to get cluster instance info.       | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:getMetadataSyncStatus       | Grants permission to get meta data sync status.       | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:startMetadataSync           | Grants permission to start meta data sync.            | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:stopMetadataSync            | Grants permission to stop meta data sync.             | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                           | Description                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                                         |
|----------------------------------|----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| dws:cluster:updatePeriodCluster  | Grants permission to update period cluster.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:periodCluster:modify</li> </ul>  |
| dws:cluster:createPeriodCluster  | Grants permission to create period cluster.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:periodCluster:create</li> </ul>  |
| dws:cluster:deleteConfigTemplate | Grants permission to delete config template. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• dws:parameterGroup:delete</li> </ul> |
| dws:cluster:getCountDown         | Grants permission to get count down.         | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                             |
| dws:cluster:getObsHotStorage     | Grants permission to get obs hot storage.    | Read         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                             |
| dws:cluster:listConfigTemplate   | Grants permission to list config template.   | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                             |



| Action                       | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                          |
|------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| dws:cluster:listDwsResource  | Grants permission to list dws resource.                               | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:resources:list           |
| dws:cluster:listDiscountNode | Grants permission to list discount node.                              | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| dws:cluster:changeToPeriod   | Grants permission to change to period.                                | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:ondemandToPeriod:operate |
| dws:cluster:rotateKey        | Grants permission to rotate key.                                      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| dws:cluster:operateCluster   | Grants permission to operate cluster, such as repair/cancel readonly. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                              |
| dws:cluster:doUpgrade        | Grants permission to do upgrade.                                      | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:cluster:doUpdate         |

| Action                         | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                           |
|--------------------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| dws:cluster:listUpgradePath    | Grants permission to list upgrade path.     | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:cluster:getUpgradePaths   |
| dws:cluster:listUpgradeRecord  | Grants permission to list upgrade record.   | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dws:cluster:getUpgradeRecords |
| dws:cluster:createDatabaseUser | Grants permission to create database user.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                               |
| dws:cluster:deleteDatabaseUser | Grants permission to delete database user.  | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                               |
| dws:cluster:getUserRoles       | Grants permission to list user roles.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                               |
| dws:cluster:getUserAuthority   | Grants permission to list user Authorities. | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                               |

| Action                               | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|--------------------------------------|---------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:getDatabaseObjects       | Grants permission to list database objects.       | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listLogicalClusterPlans  | Grants permission to list logical cluster plans.  | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:createLogicalClusterPlan | Grants permission to create logical cluster plan. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:deleteLogicalClusterPlan | Grants permission to delete logical cluster plan. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:listDatabaseUsers        | Grants permission to list database users.         | List         | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dws:cluster:switchLogicalClusterPlan | Grants permission to switch logical cluster plan. | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                               | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                           | Alias |
|--------------------------------------|------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dws:cluster:updateLogicalClusterPlan | Grants permission to update logical cluster plan.    | Write        | cluster *                   | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                      | -     |
| dws:migration:listBucketObject       | Grants permission to obtain a list of bucket objects | Write        | -                           | -                                                                                                                                                                                       | -     |
| dws:migration:deleteBucketObject     | Grants permission to delete bucket objects           | Write        | -                           | -                                                                                                                                                                                       | -     |
| dws:websql:listExecSqlRecord         | Grants permission to query the SQL execution records | List         | -                           | -                                                                                                                                                                                       | -     |
| dws:cluster:changeSecurityGroup      | Grants permission to change security group.          | Write        | cluster *                   | -                                                                                                                                                                                       | -     |
|                                      |                                                      |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> |       |
| dws:migration:setBucketLifecycle     | set                                                  | Write        | -                           | -                                                                                                                                                                                       | -     |
| dws:migration:setBucketEncryption    | Grants permission to set bucket encryption.          | Write        | -                           | -                                                                                                                                                                                       | -     |

| Action                             | Description                                                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dws:migration:showBucketEncryption | Grants permission to obtain a set of temporary security credentials that can be used to access bucket encryption. | Write        | -                           | -             | -     |
| dws:migration:showBucketLifecycle  | Grants permission to query the lifecycle of buckets                                                               | Write        | -                           | -             | -     |

Each API of dws usually supports one or more actions. [Table 3-198](#) lists the supported actions and dependencies.

**Table 3-198** Actions and dependencies supported by dws APIs

| API                                               | Action                       | Dependencies |
|---------------------------------------------------|------------------------------|--------------|
| POST /v2/{project_id}/alarm-subs                  | dws:alarm:createSubscription | -            |
| DELETE /v2/{project_id}/alarm-subs/{alarm_sub_id} | dws:alarm:deleteSubscription | -            |
| GET /v2/{project_id}/alarm-configs                | dws:alarm:listConfig         | -            |
| GET /v2/{project_id}/alarms                       | dws:alarm:listDetail         | -            |
| GET /v2/{project_id}/alarm-statistic              | dws:alarm:listStatistics     | -            |

| API                                                            | Action                                | Dependencies |
|----------------------------------------------------------------|---------------------------------------|--------------|
| GET /v2/{project_id}/alarm-subs                                | dws:alarm:listSubscription            | -            |
| PUT /v2/{project_id}/alarm-subs/{alarm_sub_id}                 | dws:alarm:updateSubscription          | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/cns/batch-create | dws:cluster:addCN                     | -            |
| PUT /v2/{project_id}/clusters/{cluster_id}/workload/queues     | dws:cluster:addQueueForWLM            | -            |
| POST /v2/{project_id}/clusters/{cluster_id}/eips/{eip_id}      | dws:cluster:bindEIP                   | -            |
| POST /v2/{project_id}/clusters/{cluster_id}/elbs/{elb_id}      | dws:cluster:bindELB                   | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/cancel-readonly  | dws:cluster:cancelReadOnly            | -            |
| GET /v2/{project_id}/disaster-recovery/check-name              | dws:cluster:checkDisasterRecoveryName | -            |
| POST /v1.0/{project_id}/snapshots/{snapshot_id}/linked-copy    | dws:cluster:copySnapshot              | -            |

| API                                                            | Action                       | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1.0/{project_id}/clusters                               | dws:cluster:create           | <ul style="list-style-type: none"> <li>• ecs:cloudServerQuotas:get</li> <li>• ecs:cloudServerFlavors:get</li> <li>• bms:serverQuotas:get</li> <li>• bms:serverFlavors:get</li> <li>• vpc:subnets:get</li> <li>• vpc:vpcs:list</li> <li>• vpc:ports:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> <li>• vpc:securityGroups:get</li> <li>• vpc:securityGroups:create</li> <li>• vpc:securityGroups:delete</li> <li>• vpc:securityGroupRules:create</li> <li>• vpc:securityGroupRules:delete</li> <li>• vpc:quotas:list</li> <li>• eip:publicIps:list</li> <li>• eip:publicIps:get</li> <li>• eip:publicIps:create</li> <li>• evs:quotas:get</li> </ul> |
| POST /v2/{project_id}/clusters                                 | dws:cluster:create           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| POST /v2/{project_id}/cluster-precheck                         | dws:cluster:create           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| POST /v1.0/{project_id}/clusters/{cluster_id}/dns              | dws:cluster:createConnection | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| POST /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources | dws:cluster:createDataSource | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| API                                                                                   | Action                              | Dependencies |
|---------------------------------------------------------------------------------------|-------------------------------------|--------------|
| POST /v2/{project_id}/disaster-recoveries                                             | dws:cluster:createDisasterRecovery  | -            |
| POST /v2/{project_id}/clusters/{cluster_id}/workload                                  | dws:cluster:setFunctionStatusForWLM | -            |
| POST /v1.0/{project_id}/snapshots                                                     | dws:cluster:createSnapshot          | -            |
| PUT /v2/{project_id}/clusters/{cluster_id}/snapshot-policies                          | dws:cluster:createSnapshotPolicy    | -            |
| POST /v2/{project_id}/clusters/{cluster_id}/workload/plans                            | dws:cluster:addPlanForWLM           | -            |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}                                       | dws:cluster:delete                  | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/cns/batch-delete                        | dws:cluster:deleteCN                | -            |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}/dns                                   | dws:cluster:deleteConnection        | -            |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id} | dws:cluster:deleteDataSource        | -            |



| API                                                                    | Action                             | Dependencies |
|------------------------------------------------------------------------|------------------------------------|--------------|
| DELETE /v2/{project_id}/disaster-recovery/{disaster_recovery_id}       | dws:cluster:deleteDisasterRecovery | -            |
| POST /v2/{project_id}/clusters/{cluster_id}/nodes/delete               | dws:cluster:deleteNode             | -            |
| DELETE /v1.0/{project_id}/snapshots/{snapshot_id}                      | dws:cluster:deleteSnapshot         | -            |
| DELETE /v1.0/{project_id}/clusters/{cluster_id}/snapshot-policies/{id} | dws:cluster:deleteSnapshotPolicy   | -            |
| DELETE /v2/{project_id}/clusters/{cluster_id}/workload/queues          | dws:cluster:deleteQueueForWLM      | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/expand-instance-storage  | dws:cluster:expandDisk             | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}                           | dws:cluster:getDetail              | -            |
| GET /v2/{project_id}/disaster-recoveries                               | dws:cluster:getDisasterRecovery    | -            |
| GET /v2/{project_id}/disaster-recovery/{disaster_recovery_id}          | dws:cluster:getDisasterRecovery    | -            |
| GET /v1.0/{project_id}/clusters                                        | dws:cluster:list                   | -            |

| API                                                                            | Action                           | Dependencies |
|--------------------------------------------------------------------------------|----------------------------------|--------------|
| GET /v1.0/{project_id}/clusters/{cluster_id}/audit-log-records                 | dws:cluster:listAuditLog         | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/cns                               | dws:cluster:listCN               | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/configurations                    | dws:cluster:listConfig           | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/configurations/{configuration_id} | dws:cluster:listConfig           | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources                  | dws:cluster:listDataSource       | -            |
| GET /v2/{project_id}/clusters/{cluster_id}/elbs                                | dws:cluster:listELB              | -            |
| GET /v2/{project_id}/disaster-recovery-clusters                                | dws:cluster:listDisasterRecovery | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/shrink-numbers                    | dws:cluster:listRingForScaleIn   | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/snapshots                         | dws:cluster:listSnapshot         | -            |

| API                                                                  | Action                              | Dependencies |
|----------------------------------------------------------------------|-------------------------------------|--------------|
| GET /v1.0/{project_id}/snapshots                                     | dws:cluster:listSnapshot            | -            |
| GET /v1.0/{project_id}/snapshots/{snapshot_id}                       | dws:cluster:getSnapshotDetail       | -            |
| GET /v2/{project_id}/clusters/{cluster_id}/snapshot-policies         | dws:cluster:listSnapshotPolicy      | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/snapshots/statistics    | dws:cluster:listSnapshotStatistics  | -            |
| GET /v1.0/{project_id}/clusters/{cluster_id}/tags                    | dws::listTagsForResource            | -            |
| GET /v2/{project_id}/clusters/{cluster_id}/workload                  | dws:cluster:getFunctionStatusForWLM | -            |
| GET /v2/{project_id}/clusters/{cluster_id}/workload/queues           | dws:cluster:listQueueForWLM         | -            |
| POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/pause | dws:cluster:pauseDisasterRecovery   | -            |
| POST /v2/{project_id}/clusters/{cluster_id}/redistribution           | dws:cluster:redistribution          | -            |

| API                                                                     | Action                            | Dependencies |
|-------------------------------------------------------------------------|-----------------------------------|--------------|
| POST /v1.0/{project_id}/clusters/{cluster_id}/reset-password            | dws:cluster:resetPassword         | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/resize                    | dws:cluster:resize                | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/restart                   | dws:cluster:restart               | -            |
| POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/recovery | dws:cluster:restoreDisaster       | -            |
| POST /v1.0/{project_id}/snapshots/{snapshot_id}/actions                 | dws:cluster:restoreSnapshot       | -            |
| POST /v1/{project_id}/clusters/{cluster_id}/description                 | dws:cluster:saveDescriptionInfo   | -            |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/maintenance-window         | dws:cluster:setMaintenanceWindow  | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/cluster-shrink            | dws:cluster:scaleIn               | -            |
| POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/start    | dws:cluster:startDisasterRecovery | -            |

| API                                                                          | Action                                 | Dependencies |
|------------------------------------------------------------------------------|----------------------------------------|--------------|
| POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/failover      | dws:cluster:switchFailoverDisaster     | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/switchover                     | dws:cluster:switchover                 | -            |
| POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/switchover    | dws:cluster:switchoverDisasterRecovery | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/tags/batch-create              | dws::tagResource                       | -            |
| DELETE /v2/{project_id}/clusters/{cluster_id}/eips/{eip_id}                  | dws:cluster:unbindEIP                  | -            |
| DELETE /v2/{project_id}/clusters/{cluster_id}/elbs/{elb_id}                  | dws:cluster:unbindELB                  | -            |
| POST /v1.0/{project_id}/clusters/{cluster_id}/tags/batch-delete              | dws::unTagResource                     | -            |
| PUT /v2/{project_id}/clusters/{cluster_id}/configurations/{configuration_id} | dws:cluster:updateConfig               | -            |
| PUT /v1.0/{project_id}/clusters/{cluster_id}/dns                             | dws:cluster:updateConnection           | -            |

| API                                                                                | Action                                   | Dependencies |
|------------------------------------------------------------------------------------|------------------------------------------|--------------|
| PUT /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id} | dws:cluster:updateDataSource             | -            |
| PUT /v2/{project_id}/disaster-recovery/{disaster_recovery_id}                      | dws:cluster:updateDisasterRecoveryConfig | -            |
| POST /v2/{project_id}/event-subs                                                   | dws:event:createSubscription             | -            |
| DELETE /v2/{project_id}/event-subs/{event_sub_id}                                  | dws:event:deleteSubscription             | -            |
| GET /v2/{project_id}/events                                                        | dws:event:list                           | -            |
| GET /v2/{project_id}/event-specs                                                   | dws:event:listSpec                       | -            |
| GET /v2/{project_id}/event-subs                                                    | dws:event:listSubscription               | -            |
| PUT /v2/{project_id}/event-subs/{event_sub_id}                                     | dws:event:updateSubscription             | -            |
| GET /v1.0/{project_id}/availability-zones                                          | dws:service:listAZ                       | -            |
| GET /v1.0/{project_id}/dss-pools                                                   | dws:service:listDssPools                 | -            |
| GET /v1.0/{project_id}/dms/disk                                                    | dws:monitor:listHostDisk                 | -            |
| GET /v1.0/{project_id}/dms/net                                                     | dws:monitor:listHostNet                  | -            |

| API                                                                                 | Action                               | Dependencies |
|-------------------------------------------------------------------------------------|--------------------------------------|--------------|
| GET /v1.0/{project_id}/dms/host-overview                                            | dws:monitor:listClusterOverview      | -            |
| GET /v1.0/{project_id}/job/{job_id}                                                 | dws:service:listJobDetail            | -            |
| GET /v1.0/{project_id}/dms/metric-data                                              | dws:monitor:listMonitorIndicatorData | -            |
| GET /v1.0/{project_id}/dms/metric-data/indicators                                   | dws:monitor:listMonitorIndicators    | -            |
| GET /v1.0/{project_id}/quotas                                                       | dws:service:listQuotas               | -            |
| GET /v2/{project_id}/node-types                                                     | dws:service:listSpec                 | -            |
| GET /v1.0/{project_id}/statistics                                                   | dws:service:listStatistics           | -            |
| GET /v1.0/{project_id}/tags                                                         | dws::listTagsForProject              | -            |
| POST /v2/{project_id}/clusters/{cluster_id}/logical-clusters                        | dws:cluster:createLogicalCluster     | -            |
| DELETE /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id} | dws:cluster:deleteLogicalCluster     | -            |
| PUT /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}    | dws:cluster:updateLogicalCluster     | -            |

| API                                                                                                               | Action                                  | Dependencies |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------|
| POST /v2/<br>{project_id}/<br>clusters/<br>{cluster_id}/logical-<br>clusters/<br>{logical_cluster_id}/<br>restart | dws:cluster:restartLogicalCl<br>uster   | -            |
| POST /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/sync-iam-<br>user                          | dws:cluster:synclamUser                 | -            |
| GET /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/users                                       | dws:cluster:listDatabaseUse<br>r        | -            |
| GET /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/users/<br>{name}                            | dws:cluster:getDatabaseUse<br>r         | -            |
| POST /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/users/<br>{name}                           | dws:cluster:updateDatabase<br>UserInfo  | -            |
| POST /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/authority                                  | dws:cluster:updateDatabase<br>Authority | -            |
| GET /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/authority                                   | dws:cluster:getDatabaseAut<br>hority    | -            |
| GET /v1/<br>{project_id}/<br>disaster-recovery/<br>{disaster_recovery_i<br>d}/show-progress                       | dws:cluster:getDisasterProg<br>ress     | -            |



| API                                                                          | Action                                  | Dependencies |
|------------------------------------------------------------------------------|-----------------------------------------|--------------|
| GET /v1/{project_id}/clusters/{cluster_id}/db-manager/om-user/status         | dws:cluster:getDatabaseOmUserStatus     | -            |
| POST /v1/{project_id}/clusters/{cluster_id}/db-manager/om-user/action        | dws:cluster:executeDatabaseOmUserAction | -            |
| POST /v1/{project_id}/clusters/{cluster_id}/rotate-key                       | dws:cluster:rotateKey                   | -            |
| POST /v1/{project_id}/clusters/{cluster_id}/db-manager/users                 | dws:cluster:createDatabaseUser          | -            |
| DELETE /v1/{project_id}/clusters/{cluster_id}/db-manager/users/{name}        | dws:cluster:deleteDatabaseUser          | -            |
| GET /v1/{project_id}/clusters/{cluster_id}/db-manager/users/{name}/authority | dws:cluster:getUserAuthority            | -            |
| GET /v1/{project_id}/clusters/{cluster_id}/db-manager/objects                | dws:cluster:getDatabaseObjects          | -            |
| GET /v1/{project_id}/clusters/{cluster_id}/logical-cluster-plans             | dws:cluster:listLogicalClusterPlans     | -            |

| API                                                                                                         | Action                               | Dependencies |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| POST /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/logical-<br>cluster-plans                           | dws:cluster:createLogicalClusterPlan | -            |
| DELETE /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/logical-<br>cluster-plans/<br>{plan_id}           | dws:cluster:deleteLogicalClusterPlan | -            |
| PUT /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/logical-<br>cluster-plans/<br>{plan_id}              | dws:cluster:updateLogicalClusterPlan | -            |
| PUT /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/<br>security-group                                   | dws:cluster:changeSecurityGroup      | -            |
| GET /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/users/<br>{name}/authority/<br>export | dws:cluster:getUserAuthority         | -            |
| GET /v1/<br>{project_id}/<br>clusters/<br>{cluster_id}/db-<br>manager/users/<br>export                      | dws:cluster:listDatabaseUser         | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-199](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for dws.

**Table 3-199** Resource types supported by dws

| Resource Type | URN                                            |
|---------------|------------------------------------------------|
| cluster       | dws:<region>:<account-id>:cluster:<cluster-id> |

## Conditions

dws does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.10 Middleware

### 3.10.1 Cloud Service Engine CSE

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set permissions boundaries for the entity. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.

- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN for the Resource element in your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CSE, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CSE, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CSE.

**Table 3-200** Supported actions

| Action              | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias             |
|---------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------|
| cse:config:upload   | Assigning permissions to upload microservice configurations   | write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cse:config:modify |
| cse:config:download | Assigning permissions to download microservice configurations | write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cse:config:modify |

| Action               | Description                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                           | Alias               |
|----------------------|-----------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| cse:namespace:list   | Assigning permissions to view the namespace resource list | list         | -                           | -                                                                                                                                                                                       | cse:namespace:read  |
| cse:namespace:get    | Assigning permissions to view namespaces                  | read         | engine                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                      | cse:namespace:read  |
| cse:namespace:create | Assigning permissions to create a namespace               | write        | engine                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | cse:namespace:write |
| cse:namespace:update | Assigning permissions to modify namespace resources       | write        | engine                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                      | cse:namespace:write |
| cse:namespace:delete | Assigning permissions to delete a namespace               | write        | engine                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                      | cse:namespace:write |
| cse:policy:list      | Assigning permissions to view the governance policy list  | list         | -                           | -                                                                                                                                                                                       | cse:governance:get  |
| cse:policy:get       | Assigning permissions to view governance policies         | read         | -                           | -                                                                                                                                                                                       | -                   |

| Action                        | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                 | Alias                 |
|-------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| cse:policy:create             | Assigning permissions to create a governance policy                                             | write        | -                           | -                                                                                                                                                             | cse:governance:modify |
| cse:policy:update             | Assigning permissions to modify governance policies                                             | write        | -                           | -                                                                                                                                                             | cse:governance:modify |
| cse:policy:delete             | Assigning permissions to delete a governance policy                                             | write        | -                           | -                                                                                                                                                             | cse:governance:modify |
| cse:engine:get                | Assigning permissions to view engines                                                           | read         | engine                      | <ul style="list-style-type: none"> <li><i><a href="#">g:Resource Tag/&lt;tag-key&gt;</a></i></li> <li><i><a href="#">g:EnterpriseProjectId</a></i></li> </ul> | -                     |
| cse:engine:list               | Assigning permissions to view the engine list                                                   | list         | -                           | -                                                                                                                                                             | -                     |
| cse:engine:backupRecover      | Assigning permissions to back up and restore ServiceComb engine data and change backup policies | write        | engine                      | <ul style="list-style-type: none"> <li><i><a href="#">g:Resource Tag/&lt;tag-key&gt;</a></i></li> <li><i><a href="#">g:EnterpriseProjectId</a></i></li> </ul> | -                     |
| cse:engine:associatePublicips | Assigning permissions to bind or unbind a ServiceComb engine to or from a public network        | write        | engine                      | <ul style="list-style-type: none"> <li><i><a href="#">g:Resource Tag/&lt;tag-key&gt;</a></i></li> <li><i><a href="#">g:EnterpriseProjectId</a></i></li> </ul> | -                     |

| Action                 | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                     | Alias             |
|------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| cse:engine:update      | Assigning permissions to modify the ServiceComb engine configuration and system management | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                    | -                 |
| cse:engine:resize      | Assigning permissions to change ServiceComb engine specifications                          | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                    | -                 |
| cse:engine:create      | Assigning permissions to create an engine                                                  | write        | -                           | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | -                 |
| cse:engine:upgrade     | Assigning permissions to upgrade engine permissions                                        | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                    | -                 |
| cse:engine:delete      | Assigning permissions to deleting an engine                                                | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                    | -                 |
| cse:engine:tagResource | Assigning permissions to add engine tags                                                   | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                    | cse:engine:modify |

| Action                         | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias             |
|--------------------------------|------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| cse:engine:unTagResource       | Assigning permissions to delete engine tags                | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | cse:engine:modify |
| cse:engine:listTags            | Assigning permissions to view all engine tags of a project | list         | -                           | -                                                                                                                                              | cse:engine:list   |
| cse:engine:listTagsForResource | Assigning permissions to view engine tags                  | list         | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | cse:engine:get    |
| cse:engine:listResourcesByTag  | Assigning permissions to query the engine list by tag      | list         | -                           | <a href="#">g:TagKeys</a>                                                                                                                      | cse:engine:list   |

Each API of CSE usually supports one or more actions. [Table 3-201](#) lists the actions and dependencies supported by CSE APIs.

**Table 3-201** Actions and dependencies supported by CSE APIs

| API                                                              | Action            | Dependencies |
|------------------------------------------------------------------|-------------------|--------------|
| GET /v2/{project_id}/enginemgr/engines/{engine_id}               | cse:engine:get    | -            |
| PUT /v2/{project_id}/enginemgr/engines/{engine_id}/actions       | cse:engine:update | -            |
| GET /v2/{project_id}/enginemgr/engines/{engine_id}/jobs/{job_id} | cse:engine:get    | -            |
| GET /v2/{project_id}/enginemgr/engines                           | cse:engine:list   | -            |



| API                                                             | Action                 | Dependencies |
|-----------------------------------------------------------------|------------------------|--------------|
| POST /v3/{project_id}/accounts/{name}/password                  | cse:engine:update      | -            |
| POST /v1/{project_id}/kie/download                              | cse:config:download    | -            |
| POST /v1/{project_id}/kie/file                                  | cse:config:upload      | -            |
| GET /v1/{project_id}/kie/kv                                     | cse:namespace:get      | -            |
| POST /v1/{project_id}/kie/kv                                    | cse:namespace:update   | -            |
| DELETE /v1/{project_id}/kie/kv                                  | cse:namespace:update   | -            |
| PUT /v1/{project_id}/kie/kv/{kv_id}                             | cse:namespace:update   | -            |
| DELETE /v1/{project_id}/kie/kv/{kv_id}                          | cse:namespace:update   | -            |
| GET /v1/{project_id}/nacos/v1/console/namespaces                | cse:namespace:get      | -            |
| DELETE /v1/{project_id}/nacos/v1/console/namespaces             | cse:namespace:delete   | -            |
| POST /v1/{project_id}/nacos/v1/console/namespaces               | cse:namespace:create   | -            |
| PUT /v1/{project_id}/nacos/v1/console/namespaces                | cse:namespace:update   | -            |
| POST /v2/{project_id}/{resource_type}/{resource_id}/tags/create | cse:engine:tagResource | -            |
| POST /v2/{project_id}/enginemgr/engines                         | cse:engine:create      | -            |
| GET /v2/{project_id}/enginemgr/engines/{engine_id}              | cse:engine:get         | -            |

| API                                                                                | Action             | Dependencies |
|------------------------------------------------------------------------------------|--------------------|--------------|
| DELETE /v2/{project_id}/<br>enginemgr/engines/<br>{engine_id}                      | cse:engine:delete  | -            |
| PUT /v2/{project_id}/<br>enginemgr/engines/<br>{engine_id}/resize                  | cse:engine:resize  | -            |
| PUT /v2/{project_id}/<br>enginemgr/engines/<br>{engine_id}/config                  | cse:engine:update  | -            |
| PUT /v2/{project_id}/<br>enginemgr/engines/<br>{engine_id}/upgrade                 | cse:engine:upgrade | -            |
| DELETE /v3/{project_id}/<br>accounts/{name}                                        | cse:engine:update  | -            |
| PUT /v3/{project_id}/<br>accounts/{name}                                           | cse:engine:modify  | -            |
| GET /v3/{project_id}/<br>govern/governance/<br>{kind}                              | cse:policy:list    | -            |
| POST /v3/{project_id}/<br>govern/governance/<br>{kind}                             | cse:policy:create  | -            |
| DELETE /v3/{project_id}/<br>govern/governance/<br>{kind}/{policy_id}               | cse:policy:delete  | -            |
| GET /v3/{project_id}/<br>govern/governance/<br>{kind}/{policy_id}                  | cse:policy:get     | -            |
| PUT /v3/{project_id}/<br>govern/governance/<br>{kind}/{policy_id}                  | cse:policy:update  | -            |
| GET /v3/{project_id}/<br>govern/governance/<br>display                             | cse:policy:list    | -            |
| DELETE /v3/{project_id}/<br>govern/route-rule/<br>microservices/<br>{service_name} | cse:policy:delete  | -            |

| API                                                                             | Action            | Dependencies |
|---------------------------------------------------------------------------------|-------------------|--------------|
| PUT /v3/{project_id}/<br>govern/route-rule/<br>microservices/<br>{service_name} | cse:policy:update | -            |
| GET /v3/{project_id}/<br>govern/route-rule/<br>microservices/<br>{service_name} | cse:policy:get    | -            |
| POST /cseengine/v1/<br>engines/{engine_id}/<br>backups/{backup_id}/<br>recovery | cse:engine:create | -            |
| POST /cseengine/v1/<br>engines/{engineId}/<br>backup-strategies                 | cse:engine:create | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-202](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an SCP to define resource types.

The following table lists the resource types that you can define in SCP statements for CSE.

**Table 3-202** Resource types supported by CSE

| Resource Type | URN                                                            |
|---------------|----------------------------------------------------------------|
| namespace     | cse:<region>:<account-id>:namespace:<engine-id>/<namespace-id> |
| policy        | cse:<region>:<account-id>;policy:<namespace-id>/<policy-name>  |
| engine        | cse:<region>:<account-id>;engine:<engine-id>                   |

## Conditions

CSE does not support service-specific condition keys in policies.

It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.10.2 Distributed Message Service for Kafka (Kafka)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DMS for Kafka, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.

- If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
- If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DMS for Kafka, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DMS for Kafka.

**Table 3-203** Actions supported by DMS for Kafka

| Action                             | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dms:instance:connector             | Grants permission to enable instance connector feature. | Write        | kafka *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dms:instance:list                  | Grants permission to query instance list.               | List         | kafka *                     | <a href="#">g:EnterpriseProjectId</a>                                                                                                              | -     |
| dms:instance:scale                 | Grants permission to scale up instance.                 | Write        | kafka *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dms:instance:listConnectorSinkTask | Grants permission to query connector sink task list.    | List         | kafka *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                            | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                              | Alias                                                                   |
|-----------------------------------|--------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| dms:instance:getBackgroundTask    | Grants permission to query instance background tasks.  | Read         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                         | -                                                                       |
| dms:instance:deleteBackgroundTask | Grants permission to delete instance background tasks. | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                         | -                                                                       |
| dms:instance:create               | Grants permission to create instance.                  | Write        | kafka*                      | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">dms:ssl</a></li> <li>• <a href="#">dms:publicIp</a></li> <li>• <a href="#">dms:connector</a></li> </ul> | -                                                                       |
| dms:instance:update               | Grants permission to modify instance.                  | Write        | kafka*                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                            | <ul style="list-style-type: none"> <li>• dms:instance:modify</li> </ul> |

| Action                               | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|--------------------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| dms:instance:upgrade                 | Grants permission to upgrade instance.                   | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
| dms:instance:getDetail               | Grants permission to query instance detail information.  | Read         | kafka*                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:get    |
| dms:instance:closeManager            | Grants permission to close kafka manager.                | Write        | kafka*                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |
| dms:instance:deleteConnectorSinkTask | Grants permission to delete connector sink task.         | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |
| dms:instance:modifyAuthInfo          | Grants permission to change access password of instance. | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |
| dms:instance:modifyStatus            | Grants permission to restart instance.                   | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |

| Action                               | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                                  |
|--------------------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------------------|
| dms:instance:delete                  | Grants permission to delete instance.                   | Write        | kafka*                      | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -                                      |
| dms:instance:getConnectorSinkTask    | Grants permission to query connector sink task.         | Read         | kafka                       | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -                                      |
| dms:instance:createConnectorSinkTask | Grants permission to create connector sink task.        | Write        | kafka                       | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -                                      |
| dms:instance:updateConnectorSinkTask | Grants permission to update connector sink task.        | Write        | kafka                       | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | • dms:instance:createConnectorSinkTask |
| dms:instance:resetAuthInfo           | Grants permission to reset access password of instance. | Write        | kafka                       | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -                                      |
| dms:message:get                      | Grants permission to query message detail.              | Read         | kafka                       | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | • dms:instance:get                     |
|                                      |                                                         |              | topic                       | -                                                                                                              |                                        |



| Action                         | Description                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|--------------------------------|--------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| dms:message:send               | Grants permission to send message.         | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
| dms:topic:list                 | Grants permission to query topic list.     | List         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:get    |
|                                |                                            |              | topic *                     | -                                                                                                                                                  |                       |
| dms:topic:modify               | Grants permission to modify topics.        | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
|                                |                                            |              | topic *                     | -                                                                                                                                                  |                       |
| dms:topic:create               | Grants permission to create topics.        | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
|                                |                                            |              | topic                       | -                                                                                                                                                  |                       |
| dms:instance:getTopicDiskUsage | Grants permission to get topic disk usage. | Read         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |

| Action                    | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|---------------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| dms:topic:delete          | Grants permission to delete topics.                      | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
|                           |                                                          |              | topic *                     | -                                                                                                                                                  |                       |
| dms:topic:getAccessPolicy | Grants permission to get topic access policy.            | Read         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:get    |
|                           |                                                          |              | topic *                     | -                                                                                                                                                  |                       |
| dms:topic:autoCreate      | Grants permission to enable or disable topic autoCreate. | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
| dms:topic:get             | Grants permission to query topic detail.                 | Read         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:get    |
|                           |                                                          |              | topic *                     | -                                                                                                                                                  |                       |
| dms:topic:updateReplica   | Grants permission to update topic partition replica.     | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |
|                           |                                                          |              | topic *                     | -                                                                                                                                                  |                       |

| Action                    | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|---------------------------|-----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| dms:topic:setAccessPolicy | Grants permission to set access policy for topic.               | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
|                           |                                                                 |              | topic*                      | -                                                                                                                                                  |                       |
| dms:user:list             | Grants permission to list users of instance.                    | List         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:get    |
| dms:user:modify           | Grants permission to modify instance users.                     | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
| dms:user:delete           | Grants permission to delete instance user.                      | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
| dms:user:create           | Grants permission to create instance users.                     | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
| dms:group:get             | Grants permission to get consumer group's detailed information. | Read         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:get    |

| Action           | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                       |
| dms:group:list   | Grants permission to list consumer groups.  | List         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:get    |
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                       |
| dms:group:modify | Grants permission to modify consumer group. | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                       |
| dms:group:create | Grants permission to create consumer group. | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                       |

| Action                     | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|----------------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| dms:group:delete           | Grants permission to delete consumer group.        | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |
|                            |                                                    |              | consumerGroup*              | -                                                                                                                                                  |                       |
| dms:coordinator:list       | Grants permission to get coordinators of instance. | List         | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |
| dms:instance:reassignTopic | Grants permission to reassign topic.               | Write        | kafka*                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                     |
| dms::updateRecyclePolicy   | Grants permission to update recycle policy.        | Write        | -                           | -                                                                                                                                                  | • dms:instance:modify |
| dms:instance:restore       | Grants permission to restore instance.             | Write        | kafka                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dms:instance:modify |

Each API of DMS for Kafka usually supports one or more actions. [Table 3-204](#) lists the supported actions and dependencies.

**Table 3-204** Actions and dependencies supported by DMS for Kafka APIs

| API                                                                 | Action                      | Dependencies |
|---------------------------------------------------------------------|-----------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/messages               | dms:message:get             | -            |
| PUT /v2/{project_id}/instances/{instance_id}/kafka-manager-password | dms:instance:modifyAuthInfo | -            |
| PUT /v2/{project_id}/instances/{instance_id}/restart-kafka-manager  | dms:instance:modifyStatus   | -            |
| DELETE /v2/{project_id}/kafka/instances/{instance_id}/management    | dms:instance:closeManager   | -            |
| POST /v2/{project_id}/instances/action                              | dms:instance:delete         | -            |
| GET /v2/{project_id}/instances                                      | dms:instance:list           | -            |
| POST /v2/{project_id}/kafka/instances/{instance_id}/extend          | dms:instance:scale          | -            |
| GET /v2/{project_id}/kafka/instances/{instance_id}/extend           | dms:instance:getDetail      | -            |

| API                                                           | Action                               | Dependencies                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/instances/{instance_id}/connector       | dms:instance:connector               | <ul style="list-style-type: none"> <li>• vpc:vpcs:get</li> <li>• vpc:vpcs:list</li> <li>• vpc:ports:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> <li>• vpc:ports:delete</li> <li>• vpc:securityGroups:get</li> <li>• vpc:subnets:get</li> <li>• eip:publicIps:get</li> <li>• eip:publicIps:list</li> <li>• eip:publicIps:update</li> </ul> |
| GET /v2/{project_id}/instances/{instance_id}                  | dms:instance:getDetail               | <ul style="list-style-type: none"> <li>• vpc:vpcs:get</li> <li>• vpc:ports:get</li> <li>• vpc:securityGroups:get</li> <li>• vpc:subnets:get</li> <li>• eip:publicIps:get</li> </ul>                                                                                                                                                                            |
| PUT /v2/{project_id}/instances/{instance_id}                  | dms:instance:update                  | <ul style="list-style-type: none"> <li>• vpc:vpcs:get</li> <li>• vpc:subnets:get</li> <li>• eip:publicIps:get</li> <li>• eip:publicIps:update</li> <li>• vpc:ports:get</li> <li>• vpc:securityGroups:get</li> <li>• vpc:securityGroups:update</li> </ul>                                                                                                       |
| POST /v2/{project_id}/kafka/instances/{instance_id}/upgrade   | dms:instance:upgrade                 | -                                                                                                                                                                                                                                                                                                                                                              |
| DELETE /v2/{project_id}/instances/{instance_id}               | dms:instance:delete                  | -                                                                                                                                                                                                                                                                                                                                                              |
| POST /v2/{project_id}/instances/{instance_id}/connector/tasks | dms:instance:createConnectorSinkTask | -                                                                                                                                                                                                                                                                                                                                                              |

| API                                                                           | Action                               | Dependencies |
|-------------------------------------------------------------------------------|--------------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/connector/tasks                  | dms:instance:listConnectorSinkTask   | -            |
| PUT /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}/pause  | dms:instance:updateConnectorSinkTask | -            |
| PUT /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}/resume | dms:instance:updateConnectorSinkTask | -            |
| GET /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}        | dms:instance:getConnectorSinkTask    | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/connector/tasks/{task_id}     | dms:instance:deleteConnectorSinkTask | -            |
| POST /v2/{project_id}/instances/{instance_id}/password                        | dms:instance:resetAuthInfo           | -            |
| GET /v2/{project_id}/instances/{instance_id}/tasks                            | dms:instance:getBackgroundTask       | -            |
| GET /v2/{project_id}/instances/{instance_id}/tasks/{task_id}                  | dms:instance:getBackgroundTask       | -            |



| API                                                             | Action                            | Dependencies |
|-----------------------------------------------------------------|-----------------------------------|--------------|
| DELETE /v2/{project_id}/instances/{instance_id}/tasks/{task_id} | dms:instance:deleteBackgroundTask | -            |
| GET /v2/{project_id}/instances/{instance_id}/topics             | dms:topic:list                    | -            |
| PUT /v2/{project_id}/instances/{instance_id}/topics             | dms:topic:modify                  | -            |
| POST /v2/{project_id}/instances/{instance_id}/topics            | dms:topic:create                  | -            |
| GET /v2/{project_id}/instances/{instance_id}/topics/diskusage   | dms:instance:getTopicDiskUsage    | -            |
| POST /v2/{project_id}/instances/{instance_id}/topics/delete     | dms:topic:delete                  | -            |
| POST /v2/{project_id}/instances/{instance_id}/crossvpc/modify   | dms:instance:update               | -            |
| GET /v2/{project_id}/instances/{instance_id}/users              | dms:user:list                     | -            |
| PUT /v2/{project_id}/instances/{instance_id}/users              | dms:user:delete                   | -            |
| POST /v2/{project_id}/instances/{instance_id}/users             | dms:user:create                   | -            |

| API                                                                                                                                             | Action                 | Dependencies |
|-------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--------------|
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/users/<br>{user_name}                                                                  | dms:user:modify        | -            |
| POST /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>autotopic                                                                         | dms:topic:autoCreate   | -            |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>management/<br>topics/{topic}/<br>partitions/<br>{partition}/<br>beginning-message | dms:message:get        | -            |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>management/<br>topics/{topic}/<br>partitions/<br>{partition}/end-<br>message       | dms:message:get        | -            |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>management/<br>cluster                                                             | dms:instance:getDetail | -            |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>management/<br>groups/{group}                                                      | dms:group:get          | -            |

| API                                                                                                   | Action                  | Dependencies |
|-------------------------------------------------------------------------------------------------------|-------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/management/topics/{topic}/partitions/{partition}/message | dms:message:get         | -            |
| GET /v2/{project_id}/instances/{instance_id}/management/topics/{topic}/messages                       | dms:message:get         | -            |
| GET /v2/{project_id}/instances/{instance_id}/management/coordinators                                  | dms:coordinator:list    | -            |
| POST /v2/{project_id}/instances/{instance_id}/management/topics/{topic}/replicas-reassignment         | dms:topic:updateReplica | -            |
| GET /v2/{project_id}/instances/{instance_id}/groups                                                   | dms:group:list          | -            |

| API                                                                                               | Action                     | Dependencies                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/<br>{project_id}/kafka/<br>instances                                                     | dms:instance:create        | <ul style="list-style-type: none"> <li>• vpc:vpcs:get</li> <li>• vpc:vpcs:list</li> <li>• vpc:ports:get</li> <li>• vpc:ports:create</li> <li>• vpc:ports:update</li> <li>• vpc:ports:delete</li> <li>• vpc:securityGroups:get</li> <li>• vpc:subnets:get</li> <li>• eip:publicIps:get</li> <li>• eip:publicIps:list</li> <li>• eip:publicIps:update</li> </ul> |
| GET /v1/<br>{project_id}/<br>instances/<br>{instance_id}/topics/<br>{topic_name}/<br>accesspolicy | dms:topic:getAccessPolicy  | -                                                                                                                                                                                                                                                                                                                                                              |
| POST /v1/<br>{project_id}/<br>instances/<br>{instance_id}/topics/<br>accesspolicy                 | dms:topic:setAccessPolicy  | -                                                                                                                                                                                                                                                                                                                                                              |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/ces-<br>hierarchy                        | dms:instance:getDetail     | -                                                                                                                                                                                                                                                                                                                                                              |
| GET /v2/<br>{project_id}/kafka/<br>{instance_id}/tags                                             | dms:instance:getDetail     | -                                                                                                                                                                                                                                                                                                                                                              |
| GET /v2/<br>{project_id}/kafka/<br>tags                                                           | dms:instance:getDetail     | -                                                                                                                                                                                                                                                                                                                                                              |
| POST /v2/<br>{project_id}/kafka/<br>{instance_id}/tags/<br>action                                 | dms:instance:update        | -                                                                                                                                                                                                                                                                                                                                                              |
| POST /v2/<br>{project_id}/kafka/<br>instances/<br>{instance_id}/<br>reassign                      | dms:instance:reassignTopic | -                                                                                                                                                                                                                                                                                                                                                              |

| API                                                                          | Action                   | Dependencies |
|------------------------------------------------------------------------------|--------------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/groups/batch-delete            | dms:group:delete         | -            |
| POST /v2/{project_id}/kafka/instances/{instance_id}/group                    | dms:group:create         | -            |
| PUT /v2/{engine}/{project_id}/instances/{instance_id}/groups/{group}         | dms:group:modify         | -            |
| POST /v2/{project_id}/kafka/instances/{instance_id}/delete-connector         | dms:instance:connector   | -            |
| POST /v2/{project_id}/instances/{instance_id}/messages/action                | dms:message:send         | -            |
| GET /v2/{project_id}/kafka/instances/{instance_id}/topics/{topic}/partitions | dms:topic:get            | -            |
| GET /v2/{project_id}/kafka/instances/{instance_id}/topics/{topic}/producers  | dms:topic:get            | -            |
| PUT /v2/{engine}/{project_id}/instances/{instance_id}/users/{user_name}      | dms:user:modify          | -            |
| POST /v2/{project_id}/recycle                                                | dms:instance:restore     | -            |
| PUT /v2/{project_id}/recycle                                                 | dms::updateRecyclePolicy | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-205](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DMS for Kafka.

**Table 3-205** Resource types supported by DMS for Kafka

| Resource Type | URN                                                                        |
|---------------|----------------------------------------------------------------------------|
| kafka         | dms:<region>:<account-id>:kafka:<instance-id>                              |
| topic         | dms:<region>:<account-id>:topic:<instance-id>/<topic-name>                 |
| consumerGroup | dms:<region>:<account-id>:consumerGroup:<instance-id>/<consumerGroup-name> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, dms) apply only to operations of the xx service. For details, see [Table 3-206](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when

its request conditions are met. For supported condition operators, see [operators](#).

#### Service-specific condition keys supported by DMS for Kafka

The following table lists the condition keys that you can define in identity policies for DMS for Kafka. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-206** Service-specific condition keys supported by DMS for Kafka

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                   |
|--------------------------------|---------|-------------------------------|-------------------------------------------------------------------------------|
| dms:ssl                        | boolean | Single-valued                 | Filters access based on whether the instance is enabled for SSL access.       |
| dms:publicip                   | boolean | Single-valued                 | Filters access based on whether the instance is enabled for public IP access. |
| dms:connector                  | boolean | Single-valued                 | Filters access based on whether the instance connector is enabled.            |

### 3.10.3 Distributed Message Service for RabbitMQ (RabbitMQ)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).

- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DMS for RabbitMQ, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DMS for RabbitMQ, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DMS for RabbitMQ.



**Table 3-207** Actions supported by DMS for RabbitMQ

| Action                            | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                           | Alias |
|-----------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dms:instance:list                 | Grants permission to query instance list.              | List         | rabbitmq *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                   | -     |
| dms:instance:scale                | Grants permission to scale up instance.                | Write        | rabbitmq                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                          | -     |
| dms:instance:getBackgroundTask    | Grants permission to query instance background tasks.  | Read         | rabbitmq                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                          | -     |
| dms:instance:deleteBackgroundTask | Grants permission to delete instance background tasks. | Write        | rabbitmq                    | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                          | -     |
| dms:instance:create               | Grants permission to create instance.                  | Write        | rabbitmq *                  | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">dms:ssl</a></li> <li><a href="#">dms:publicIp</a></li> </ul> | -     |

| Action                     | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                 |
|----------------------------|---------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| dms:instance:update        | Grants permission to modify instance.                   | Write        | rabbitmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • dms:instance:modify |
| dms:instance:getDetail     | Grants permission to query instance detail information. | Read         | rabbitmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                              | • dms:instance:get    |
| dms:instance:delete        | Grants permission to delete instance.                   | Write        | rabbitmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                              | -                     |
| dms:instance:resetAuthInfo | Grants permission to reset access password of instance. | Write        | rabbitmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                              | -                     |
| dms:plugin:list            | Grants permission to list plugins of instance.          | List         | rabbitmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                              | • dms:instance:list   |

| Action                  | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                                                                 |
|-------------------------|-------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| dms:plugin:modifyStatus | Grants permission to enable or disable plugins of instance. | Write        | rabbitmq                    | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | <ul style="list-style-type: none"> <li>dms:instance:modify</li> </ul> |

Each API of DMS for RabbitMQ usually supports one or more actions. [Table 3-208](#) lists the supported actions and dependencies.

**Table 3-208** Actions and dependencies supported by DMS for RabbitMQ APIs

| API                                                           | Action                 | Dependencies                                                                                                                                                              |
|---------------------------------------------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/instances/action                        | dms:instance:delete    | -                                                                                                                                                                         |
| GET /v2/{project_id}/instances                                | dms:instance:list      | -                                                                                                                                                                         |
| POST /v2/{engine}/{project_id}/instances/{instance_id}/extend | dms:instance:scale     | -                                                                                                                                                                         |
| GET /v2/{engine}/{project_id}/instances/{instance_id}/extend  | dms:instance:getDetail | -                                                                                                                                                                         |
| GET /v2/{project_id}/instances/{instance_id}                  | dms:instance:getDetail | <ul style="list-style-type: none"> <li>vpc:vpcs:get</li> <li>vpc:ports:get</li> <li>vpc:securityGroups:get</li> <li>vpc:subnets:get</li> <li>eip:publicIps:get</li> </ul> |

| API                                                             | Action                            | Dependencies                                                                                                                                                                                                                               |
|-----------------------------------------------------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /v2/{project_id}/instances/{instance_id}                    | dms:instance:update               | <ul style="list-style-type: none"> <li>vpc:vpcs:get</li> <li>vpc:subnets:get</li> <li>eip:publicIps:get</li> <li>eip:publicIps:update</li> <li>vpc:ports:get</li> <li>vpc:securityGroups:get</li> <li>vpc:securityGroups:update</li> </ul> |
| DELETE /v2/{project_id}/instances/{instance_id}                 | dms:instance:delete               | -                                                                                                                                                                                                                                          |
| POST /v2/{project_id}/instances/{instance_id}/password          | dms:instance:resetAuthInfo        | -                                                                                                                                                                                                                                          |
| GET /v2/{project_id}/instances/{instance_id}/tasks              | dms:instance:getBackgroundTask    | -                                                                                                                                                                                                                                          |
| GET /v2/{project_id}/instances/{instance_id}/tasks/{task_id}    | dms:instance:getBackgroundTask    | -                                                                                                                                                                                                                                          |
| DELETE /v2/{project_id}/instances/{instance_id}/tasks/{task_id} | dms:instance:deleteBackgroundTask | -                                                                                                                                                                                                                                          |
| GET /v2/{project_id}/instances/{instance_id}/rabbitmq/plugins   | dms:plugin:list                   | -                                                                                                                                                                                                                                          |
| PUT /v2/{project_id}/instances/{instance_id}/rabbitmq/plugins   | dms:plugin:modifyStatus           | -                                                                                                                                                                                                                                          |

| API                                                      | Action                 | Dependencies                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{engine}/{project_id}/instances                 | dms:instance:create    | <ul style="list-style-type: none"><li>• vpc:vpcs:get</li><li>• vpc:vpcs:list</li><li>• vpc:ports:get</li><li>• vpc:ports:create</li><li>• vpc:ports:update</li><li>• vpc:ports:delete</li><li>• vpc:securityGroups:get</li><li>• vpc:subnets:get</li><li>• eip:publicIps:get</li><li>• eip:publicIps:list</li><li>• eip:publicIps:update</li></ul> |
| GET /v2/{project_id}/rabbitmq/{instance_id}/tags         | dms:instance:getDetail | -                                                                                                                                                                                                                                                                                                                                                  |
| GET /v2/{project_id}/rabbitmq/tags                       | dms:instance:getDetail | -                                                                                                                                                                                                                                                                                                                                                  |
| POST /v2/{project_id}/rabbitmq/{instance_id}/tags/action | dms:instance:update    | -                                                                                                                                                                                                                                                                                                                                                  |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-209](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DMS for RabbitMQ.

**Table 3-209** Resource types supported by DMS for RabbitMQ

| Resource Type | URN                                              |
|---------------|--------------------------------------------------|
| rabbitmq      | dms:<region>:<account-id>:rabbitmq:<instance-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, dms) apply only to operations of the xx service. For details, see **Table 3-210**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

### Service-specific condition keys supported by DMS for RabbitMQ

The following table lists the condition keys that you can define in identity policies for DMS for RabbitMQ. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-210** Service-specific condition keys supported by DMS for RabbitMQ

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                   |
|--------------------------------|---------|-------------------------------|-------------------------------------------------------------------------------|
| dms:ssl                        | boolean | Single-valued                 | Filters access based on whether the instance is enabled for SSL access.       |
| dms:publicIp                   | boolean | Single-valued                 | Filters access based on whether the instance is enabled for public IP access. |

### 3.10.4 Distributed Message Service for RocketMQ (RocketMQ)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DMS for RocketMQ, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.

- If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DMS for RocketMQ, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DMS for RocketMQ.

**Table 3-211** Actions supported by DMS for RocketMQ

| Action              | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                     | Alias               |
|---------------------|-------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| dms:instance:list   | Grants permission to query instance list. | List         | rocketmq *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                             | -                   |
| dms:instance:create | Grants permission to create instance.     | Write        | rocketmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">dms:ssl</a></li> <li>• <a href="#">dms:publicIp</a></li> </ul> | -                   |
| dms:instance:update | Grants permission to modify instance.     | Write        | rocketmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                   | dms:instance:modify |



| Action                    | Description                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias               |
|---------------------------|---------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| dms:instance:getDetail    | Grants permission to query instance detail information. | Read         | rocketmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |
| dms:instance:modifyConfig | Grants permission to modify instance config.            | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                   |
| dms:instance:delete       | Grants permission to delete instance.                   | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                   |
| dms:message:export        | Grants permission to export messages.                   | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
|                           |                                                         |              | topic                       | -                                                                                                                                                  |                     |
| dms:message:get           | Grants permission to query message detail.              | Read         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |
|                           |                                                         |              | topic                       | -                                                                                                                                                  |                     |
| dms:message:getTrace      | Grants permission to query message trace.               | Read         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |

| Action           | Description                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                       | Alias               |
|------------------|----------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| dms:message:send | Grants permission to send message.     | Write        | rocke<br>tmq                | <ul style="list-style-type: none"> <li>• <a href="#">g:Resource Tag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
| dms:topic:list   | Grants permission to query topic list. | List         | rocke<br>tmq                | <ul style="list-style-type: none"> <li>• <a href="#">g:Resource Tag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |
|                  |                                        |              | topic<br>*                  | -                                                                                                                                                   |                     |
| dms:topic:modify | Grants permission to modify topics.    | Write        | rocke<br>tmq                | <ul style="list-style-type: none"> <li>• <a href="#">g:Resource Tag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
|                  |                                        |              | topic<br>*                  | -                                                                                                                                                   |                     |
| dms:topic:create | Grants permission to create topics.    | Write        | rocke<br>tmq                | <ul style="list-style-type: none"> <li>• <a href="#">g:Resource Tag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
|                  |                                        |              | topic                       | -                                                                                                                                                   |                     |
| dms:topic:delete | Grants permission to delete topics.    | Write        | rocke<br>tmq                | <ul style="list-style-type: none"> <li>• <a href="#">g:Resource Tag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
|                  |                                        |              | topic<br>*                  | -                                                                                                                                                   |                     |

| Action                        | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|-------------------------------|----------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| dms:topic:get<br>AccessPolicy | Grants permission to get topic access policy.                  | Read         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:<br>get    |
|                               |                                                                |              | topic*                      | -                                                                                                                                                  |                         |
| dms:topic:get                 | Grants permission to query topic detail.                       | Read         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:<br>get    |
|                               |                                                                |              | topic*                      | -                                                                                                                                                  |                         |
| dms:user:list                 | Grants permission to list users of instance.                   | List         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:<br>get    |
| dms:user:get                  | Grants permission to get instance user's detailed information. | Read         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:<br>get    |
| dms:user:modify               | Grants permission to modify instance users.                    | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:<br>modify |

| Action                       | Description                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias               |
|------------------------------|------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| dms:user:delete              | Grants permission to delete instance user.                       | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
| dms:user:create              | Grants permission to create instance users.                      | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
| dms:group:get                | Grants permission to get consumer group's detailed information.  | Read         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |
|                              |                                                                  |              | consumerGroup*              | -                                                                                                                                                  |                     |
| dms:group:getAccessPolicy    | Grants permission to get the access policies for consumer group. | Read         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |
|                              |                                                                  |              | consumerGroup*              | -                                                                                                                                                  |                     |
| dms:group:resetConsumeOffset | Grants permission to reset the consume offset of consumer group. | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |

| Action           | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias               |
|------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                     |
| dms:group:list   | Grants permission to list consumer groups.  | List         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                     |
| dms:group:modify | Grants permission to modify consumer group. | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                     |
| dms:group:create | Grants permission to create consumer group. | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
|                  |                                             |              | consumerGroup*              | -                                                                                                                                                  |                     |

| Action                                   | Description                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias               |
|------------------------------------------|------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| dms:group:delete                         | Grants permission to delete consumer group.          | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:modify |
|                                          |                                                      |              | consumerGroup*              | -                                                                                                                                                  |                     |
| dms:broker:list                          | Grants permission to list brokers of instance.       | List         | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | dms:instance:get    |
| dms:instance:createMetadataMigrationTask | Grants permission to create metadata migration task. | Write        | rocketmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                   |
| dms:instance:listMetadataMigrationTasks  | Grants permission to list metadata migration tasks.  | Write        | rocketmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                   |
| dms:instance:deleteMetadataMigrationTask | Grants permission to delete metadata migration task. | Write        | rocketmq *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                   |

| Action                    | Description                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------|--------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dms:instance:resendDlqMsg | Grants permission to resend Dead-Letter Queue Message. | Write        | rocketmq                    | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

Each API of DMS for RocketMQ usually supports one or more actions. [Table 3-212](#) lists the supported actions and dependencies.

**Table 3-212** Actions and dependencies supported by DMS for RocketMQ APIs

| API                                                            | Action                 | Dependencies                                                                                                                                                                        |
|----------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v2/{engine}/{project_id}/instances/{instance_id}/messages | dms:message:get        | -                                                                                                                                                                                   |
| POST /v2/{project_id}/instances/{instance_id}/messages/export  | dms:message:export     | -                                                                                                                                                                                   |
| POST /v2/{project_id}/instances/action                         | dms:instance:delete    | -                                                                                                                                                                                   |
| GET /v2/{project_id}/instances                                 | dms:instance:list      | -                                                                                                                                                                                   |
| GET /v2/{project_id}/instances/{instance_id}                   | dms:instance:getDetail | <ul style="list-style-type: none"> <li>• vpc:vpcs:get</li> <li>• vpc:ports:get</li> <li>• vpc:securityGroups:get</li> <li>• vpc:subnets:get</li> <li>• eip:publicIps:get</li> </ul> |

| API                                                               | Action               | Dependencies                                                                                                                                                                                                                               |
|-------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /v2/{project_id}/instances/{instance_id}                      | dms:instance:update  | <ul style="list-style-type: none"> <li>vpc:vpcs:get</li> <li>vpc:subnets:get</li> <li>eip:publicIps:get</li> <li>eip:publicIps:update</li> <li>vpc:ports:get</li> <li>vpc:securityGroups:get</li> <li>vpc:securityGroups:update</li> </ul> |
| DELETE /v2/{project_id}/instances/{instance_id}                   | dms:instance:delete  | -                                                                                                                                                                                                                                          |
| GET /v2/{engine}/{project_id}/instances/{instance_id}/trace       | dms:message:getTrace | -                                                                                                                                                                                                                                          |
| GET /v2/{project_id}/instances/{instance_id}/topics               | dms:topic:list       | -                                                                                                                                                                                                                                          |
| POST /v2/{project_id}/instances/{instance_id}/topics              | dms:topic:create     | dms:topic:delete                                                                                                                                                                                                                           |
| GET /v2/{project_id}/instances/{instance_id}/users                | dms:user:list        | -                                                                                                                                                                                                                                          |
| POST /v2/{project_id}/instances/{instance_id}/users               | dms:user:create      | -                                                                                                                                                                                                                                          |
| GET /v2/{project_id}/instances/{instance_id}/users/{user_name}    | dms:user:get         | -                                                                                                                                                                                                                                          |
| DELETE /v2/{project_id}/instances/{instance_id}/users/{user_name} | dms:user:delete      | -                                                                                                                                                                                                                                          |



| API                                                                                           | Action                       | Dependencies |
|-----------------------------------------------------------------------------------------------|------------------------------|--------------|
| PUT /v2/{project_id}/instances/{instance_id}/users/{user_name}                                | dms:user:modify              | -            |
| GET /v2/{project_id}/instances/{instance_id}/topics/{topic}/accesspolicy                      | dms:topic:getAccessPolicy    | -            |
| GET /v2/{engine}/{project_id}/instances/{instance_id}/groups/{group_id}/accesspolicy          | dms:group:getAccessPolicy    | -            |
| GET /v2/{project_id}/instances/{instance_id}/topics/{topic}/status                            | dms:topic:get                | -            |
| GET /v2/{project_id}/instances/{instance_id}/topics/{topic}/groups                            | dms:topic:get                | -            |
| GET /v2/{project_id}/instances/{instance_id}/groups/{group}/topics                            | dms:group:get                | -            |
| POST /v2/{engine}/{project_id}/instances/{instance_id}/groups/{group_id}/reset-message-offset | dms:group:resetConsumeOffset | -            |
| GET /v2/{project_id}/instances/{instance_id}/brokers                                          | dms:broker:list              | -            |

| API                                                                            | Action           | Dependencies     |
|--------------------------------------------------------------------------------|------------------|------------------|
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>groups            | dms:group:list   | -                |
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>groups            | dms:group:modify | -                |
| POST /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>groups           | dms:group:create | dms:group:delete |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>groups/{group}    | dms:group:get    | -                |
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>groups/{group}    | dms:group:modify | -                |
| DELETE /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>groups/{group} | dms:group:delete | -                |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/topics/<br>{topic}    | dms:topic:get    | -                |
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/topics/<br>{topic}    | dms:topic:modify | -                |
| DELETE /v2/<br>{project_id}/<br>instances/<br>{instance_id}/topics/<br>{topic} | dms:topic:delete | -                |

| API                                                                               | Action                    | Dependencies                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{engine}/{project_id}/instances                                          | dms:instance:create       | <ul style="list-style-type: none"> <li>vpc:vpcs:get</li> <li>vpc:vpcs:list</li> <li>vpc:ports:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>vpc:ports:delete</li> <li>vpc:securityGroups:get</li> <li>vpc:subnets:get</li> <li>eip:publicIps:get</li> <li>eip:publicIps:list</li> <li>eip:publicIps:update</li> </ul> |
| POST /v2/{project_id}/rocketmq/{instance_id}/tags/action                          | dms:instance:update       | -                                                                                                                                                                                                                                                                                                                                        |
| GET /v2/{project_id}/rocketmq/{instance_id}/tags                                  | dms:instance:getDetail    | -                                                                                                                                                                                                                                                                                                                                        |
| GET /v2/{project_id}/rocketmq/tags                                                | dms:instance:getDetail    | -                                                                                                                                                                                                                                                                                                                                        |
| GET /v2/rocketmq/{project_id}/instances/{instance_id}/groups/{group}/clients      | dms:group:get             | -                                                                                                                                                                                                                                                                                                                                        |
| POST /v2/{engine}/{project_id}/instances/{instance_id}/messages/deadletter-resend | dms:instance:resendDlqMsg | -                                                                                                                                                                                                                                                                                                                                        |
| POST /v2/{engine}/{project_id}/instances/{instance_id}/messages/resend            | dms:message:send          | -                                                                                                                                                                                                                                                                                                                                        |

| API                                                           | Action                                   | Dependencies |
|---------------------------------------------------------------|------------------------------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/metadata        | dms:instance:createMetadataMigrationTask | -            |
| GET /v2/{project_id}/instances/{instance_id}/metadata         | dms:instance:listMetadataMigrationTasks  | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/metadata      | dms:instance:deleteMetadataMigrationTask | -            |
| GET /v2/{project_id}/rocketmq/instances/{instance_id}/configs | dms:instance:getDetail                   | -            |
| PUT /v2/{project_id}/rocketmq/instances/{instance_id}/configs | dms:instance:modifyConfig                | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-213](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DMS for RocketMQ.

**Table 3-213** Resource types supported by DMS for RocketMQ

| Resource Type | URN                                                        |
|---------------|------------------------------------------------------------|
| topic         | dms:<region>:<account-id>:topic:<instance-id>/<topic-name> |

| Resource Type | URN                                                                        |
|---------------|----------------------------------------------------------------------------|
| consumerGroup | dms:<region>:<account-id>:consumerGroup:<instance-id>/<consumerGroup-name> |
| rocketmq      | dms:<region>:<account-id>:rocketmq:<instance-id>                           |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, dms for rocketmq) apply only to operations of the xx service. For details, see [Table 3-214](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by DMS for RocketMQ

The following table lists the condition keys that you can define in identity policies for DMS for RocketMQ. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-214** Service-specific condition keys supported by DMS for RocketMQ

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                   |
|--------------------------------|---------|-------------------------------|-------------------------------------------------------------------------------|
| dms:ssl                        | boolean | Single-valued                 | Filters access based on whether the instance is enabled for SSL access.       |
| dms:publicIp                   | boolean | Single-valued                 | Filters access based on whether the instance is enabled for public IP access. |

### 3.10.5 API Gateway (APIG)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.

- You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
- If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by apig, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by apig, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for apig.

**Table 3-215** Actions supported by apig

| Action          | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                |
|-----------------|-------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------|
| apig:acl:list   | Grants permission to query all the access control policies. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>• apig:acls:list</li> </ul>   |
| apig:acl:create | Grants permission to create an access control policy.       | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>• apig:acls:create</li> </ul> |

| Action                   | Description                                                             | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                  |
|--------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------|
| apig:acl:batch Delete    | Grants permission to delete multiple access control policies.           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:acls:delete</li> </ul>     |
| apig:acl:delete          | Grants permission to delete an access control policy.                   | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:acls:delete</li> </ul>     |
| apig:acl:get             | Grants permission to query the details of an access control policy.     | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:acls:get</li> </ul>        |
| apig:acl:update          | Grants permission to modify an access control policy.                   | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:acls:update</li> </ul>     |
| apig:api:bindAcl         | Grants permission to bind an access control policy to a specified API.  | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:bindAcls</li> </ul>   |
| apig:api:batch UnbindAcl | Grants permission to unbind multiple access control policies from APIs. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:unbindAcls</li> </ul> |
| apig:api:unbindAcl       | Grants permission to unbind an access control policy from an API.       | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:unbindAcls</li> </ul> |



| Action                                | Description                                                                                                | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                       |
|---------------------------------------|------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-----------------------------------------------------------------------------|
| apig:api:listBoundAcl                 | Grants permission to query the access control policies that have been bound to a specified API.            | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:listBoundAcls</li> </ul>   |
| apig:acl:listBoundApi                 | Grants permission to query the APIs to which an access control policy has been bound.                      | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:acls:listBoundApis</li> </ul>   |
| apig:acl:listUnboundApi               | Grants permission to query the published APIs to which an access control policy has not been bound.        | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:acls:listUnboundApis</li> </ul> |
| apig:api:bindRequestThrottling        | Grants permission to bind a request throttling policy to an API that has been published in an environment. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:bindThrottles</li> </ul>   |
| apig:api:batchUnbindRequestThrottling | Grants permission to unbind request throttling policies from APIs.                                         | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:unbindThrottles</li> </ul> |

| Action                                | Description                                                                                                 | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                            |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------------|
| apig:api:unbindRequestThrottling      | Grants permission to unbind a request throttling policy from an API.                                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:unbindThrottles</li> </ul>      |
| apig:requestThrottling:listBoundApi   | Grants permission to query the APIs to which a specified request throttling policy has been bound.          | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:listBoundApis</li> </ul>   |
| apig:api:listBoundRequestThrottling   | Grants permission to query the request throttling policies that have been bound to an API.                  | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:listBoundThrottles</li> </ul>   |
| apig:requestThrottling:listUnboundApi | Grants permission to query the self-developed APIs to which a request throttling policy has not been bound. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:listUnboundApis</li> </ul> |
| apig:apiGroup:list                    | Grants permission to query API groups.                                                                      | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:list</li> </ul>               |

| Action                                    | Description                                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------|
| apig:apiGroup:create                      | Grants permission to create an API group. An API group is an API management unit and the entry to a service. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:create</li> </ul> |
| apig:apiGroup:delete                      | Grants permission to delete an API group.                                                                    | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:delete</li> </ul> |
| apig:apiGroup:get                         | Grants permission to query the details of an API group.                                                      | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:get</li> </ul>    |
| apig:apiGroup:update                      | Grants permission to modify the attributes of an API group.                                                  | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:update</li> </ul> |
| apig:apiGroup:checkApiGroupNameExistOrNot | Grants permission to check whether the API group name exists.                                                | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:get</li> </ul>    |
| apig:api:list                             | Grants permission to query APIs to return details and publication information of the APIs.                   | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:list</li> </ul>     |
| apig:api:create                           | Grants permission to create an API.                                                                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:create</li> </ul>   |

| Action                                   | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                          |
|------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------------------------------|
| apig:api:delete                          | Grants permission to delete an API.                                                                   | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:delete</li> </ul>                             |
| apig:api:get                             | Grants permission to query the details of an API.                                                     | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:get</li> </ul>                                |
| apig:api:update                          | Grants permission to modify the information about an API.                                             | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:update</li> </ul>                             |
| apig:api:onlineOrOffline                 | Grants permission to publish an API or take an API offline.                                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:publish</li> <li>apig:apis:offline</li> </ul> |
| apig:api:batchDelete                     | Grants permission to delete multiple APIs.                                                            | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:delete</li> </ul>                             |
| apig:api:checkApiPathOrApiNameExistOrNot | Grants permission to verify the API definition, that is, whether the API path or name already exists. | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:get</li> </ul>                                |
| apig:api:debug                           | Grants permission to debug an API.                                                                    | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:debug</li> </ul>                              |

| Action                        | Description                                                                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                          |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------------------------------|
| apig:api:batchOnlineOrOffline | Grants permission to publish multiple APIs in an environment or to remove multiple APIs from the environment in which they have been published. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:publish</li> <li>apig:apis:offline</li> </ul> |
| apig:api:listHistoryVersion   | Grants permission to query the historical versions of an API.                                                                                   | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:get</li> </ul>                                |
| apig:api:switchVersion        | Grants permission to switch the version of an API.                                                                                              | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:publish</li> </ul>                            |
| apig:api:getRuntimeDefinition | Grants permission to query the runtime definition of an API in a specified environment.                                                         | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:get</li> </ul>                                |
| apig:api:deleteHistoryVersion | Grants permission to remove an effective version of an API.                                                                                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:offline</li> </ul>                            |

| Action                     | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                  |
|----------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------|
| apig:api:getHistoryVersion | Grants permission to query the details of a specified API version.           | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:get</li> </ul>        |
| apig:app:list              | Grants permission to query apps.                                             | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:list</li> </ul>       |
| apig:app:create            | Grants permission to create an app.                                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:create</li> </ul>     |
| apig:app:delete            | Grants permission to delete an app.                                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:delete</li> </ul>     |
| apig:app:get               | Grants permission to query the details of an app.                            | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:get</li> </ul>        |
| apig:app:update            | Grants permission to modify the information about an app.                    | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:update</li> </ul>     |
| apig:app:listAppCode       | Grants permission to query the AppCodes of an app.                           | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:appCodes:list</li> </ul>   |
| apig:app:createAppCode     | Grants permission to create an AppCode for an app for simple authentication. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:appCodes:create</li> </ul> |

| Action                   | Description                                                                                        | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------|
| apig:app:generateAppCode | Grants permission to generate a random AppCode.                                                    | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:appCodes:update</li> </ul> |
| apig:app:deleteAppCode   | Grants permission to delete an AppCode.                                                            | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:appCodes:delete</li> </ul> |
| apig:app:getAppCode      | Grants permission to query the details of an AppCode created for an app for simple authentication. | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:appCodes:get</li> </ul>    |
| apig:app:resetSecret     | Grants permission to reset the AppSecret of an app.                                                | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:update</li> </ul>     |
| apig:app:validate        | Grants permission to check whether an app exists.                                                  | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:get</li> </ul>        |
| apig:app:getBoundQuota   | Grants permission to query the application quota associated with a specified client application.   | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:get</li> </ul>        |

| Action                  | Description                                                                                                       | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-----------------------------------------------------------------------------|
| apig:app:bindApi        | Grants permission to bind the app to the API in the environment.                                                  | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:grantAppAccess</li> </ul>  |
| apig:app:unbindApi      | Grants permission to cancel the authorization of an app for accessing an API.                                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:revokeAppAccess</li> </ul> |
| apig:app:listBoundApi   | Grants permission to query the APIs to which a specified app has been bound.                                      | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:listBoundApis</li> </ul>   |
| apig:api:listBoundApp   | Grants permission to query the apps that have been bound to a specified API.                                      | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:listBoundApps</li> </ul>   |
| apig:app:listUnboundApi | Grants permission to query the self-developed APIs to which an app has not been bound in a specified environment. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:listUnboundApis</li> </ul> |



| Action                  | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                        |
|-------------------------|-------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------|
| apig:api:export         | Grants permission to export APIs in a specified API group.  | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:export</li> </ul>                           |
| apig:api:import         | Grants permission to import APIs.                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:import</li> </ul>                           |
| apig:asyncTask:get      | Grants permission to query the details of an async task.    | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:export</li> <li>apig:apis:import</li> </ul> |
| apig:certificate:list   | Grants permission to query the SSL certificates.            | List         | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                            |
| apig:certificate:create | Grants permission to create an SSL certificate.             | Write        | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                            |
| apig:certificate:delete | Grants permission to delete an SSL certificate.             | Write        | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                            |
| apig:certificate:get    | Grants permission to query the details about a certificate. | Read         | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                            |
| apig:certificate:update | Grants permission to modify an SSL certificate.             | Write        | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                            |

| Action                                         | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                            |
|------------------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------------|
| apig:certificate:listBoundDomain               | Grants permission to query the domain names to which an SSL certificate has been bound. | List         | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                |
| apig:certificate:batchBindDomain               | Grants permission to bind an SSL certificate to a domain name.                          | Write        | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                |
| apig:certificate:batchUnbindDomain             | Grants permission to unbind an SSL certificate from a domain name.                      | Write        | instance                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                                |
| apig:apiGroup:batchBindCertificateToDomain     | Grants permission to bind a domain name with SSL certificates.                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:bindCertificate</li> </ul>   |
| apig:apiGroup:batchUnbindCertificateFromDomain | Grants permission to unbind a domain name's SSL certificates.                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:unbindCertificate</li> </ul> |
| apig:loadBalancerChannel:list                  | Grants permission to query the VPC channels under a gateway.                            | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:list</li> </ul>          |

| Action                                           | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                     |
|--------------------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|---------------------------------------------------------------------------|
| apig:loadBalancerChannel:create                  | Grants permission to create a VPC channel from APIG to your private VPC resources. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:create</li> </ul> |
| apig:loadBalancerChannel:delete                  | Grants permission to delete a VPC channel.                                         | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:delete</li> </ul> |
| apig:loadBalancerChannel:get                     | Grants permission to query the details of a VPC channel.                           | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:get</li> </ul>    |
| apig:loadBalancerChannel:update                  | Grants permission to update the parameters of a VPC channel.                       | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:update</li> </ul> |
| apig:loadBalancerChannel:updateHealthCheckConfig | Grants permission to modify the health check configuration of a VPC channel.       | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:update</li> </ul> |
| apig:loadBalancerChannel:listServerGroup         | Grants permission to query backend server groups of a VPC channel.                 | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:get</li> </ul>    |

| Action                                             | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                      |
|----------------------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------|
| apig:loadBalanceChannel:createServerGroup          | Grants permission to adding or Updating a Backend Server Group of a VPC Channel. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:addOrUpdateMemberGroups</li> </ul> |
| apig:loadBalanceChannel:deleteServerGroup          | Grants permission to delete a backend server group of a specified VPC channel.   | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:deleteMemberGroup</li> </ul>       |
| apig:loadBalanceChannel:getServerGroup             | Grants permission to query a backend server group of a specified VPC channel.    | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:get</li> </ul>                     |
| apig:loadBalanceChannel:updateServerGroup          | Grants permission to update a backend server group of a VPC channel.             | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:updateMemberGroup</li> </ul>       |
| apig:loadBalanceChannel:listBackendServerAddress   | Grants permission to query the backend instances of a specified VPC channel.     | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:get</li> </ul>                     |
| apig:loadBalanceChannel:createBackendServerAddress | Grants permission to add backend instances to a VPC channel.                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:addInstance</li> </ul>             |

| Action                                                    | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                   |
|-----------------------------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-----------------------------------------------------------------------------------------|
| apig:loadBalancerChannel:updateBackendServerAddress       | Grants permission to update the backend instances of a specified VPC channel. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:addInstance</li> </ul>          |
| apig:loadBalancerChannel:deleteBackendServerAddress       | Grants permission to delete a backend instance from a specified VPC channel.  | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:deleteInstance</li> </ul>       |
| apig:loadBalancerChannel:batchDisableBackendServerAddress | Grants permission to disable backend servers of a VPC channel.                | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:batchDisableInstance</li> </ul> |
| apig:loadBalancerChannel:batchEnableBackendServerAddress  | Grants permission to enable backend servers of a VPC channel.                 | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:vpcChannels:batchEnableInstance</li> </ul>  |
| apig:instance:listTag                                     | Grants permission to query tags of a gateway.                                 | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:tags:list</li> </ul>                        |
| apig:api:listUnboundPlugin                                | Grants permission to query the plug-ins that can be bound to a specified API. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:listUnboundPlugins</li> </ul>          |

| Action                   | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                        |
|--------------------------|---------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------------|
| apig:api:listBoundPlugin | Grants permission to query the plug-ins bound to an API.      | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:listBoundPlugins</li> </ul> |
| apig:api:bindPlugin      | Grants permission to bind an API with plug-ins.               | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:bindPlugins</li> </ul>      |
| apig:api:unbindPlugin    | Grants permission to unbind an API's plug-ins.                | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:unbindPlugins</li> </ul>    |
| apig:plugin:list         | Grants permission to query details about a group of plug-ins. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:plugins:list</li> </ul>          |
| apig:plugin:create       | Grants permission to create a Plug-in.                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:plugins:create</li> </ul>        |
| apig:plugin:delete       | Grants permission to delete a plug-in.                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:plugins:delete</li> </ul>        |
| apig:plugin:get          | Grants permission to query the details of a plug-in.          | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:plugins:get</li> </ul>           |
| apig:plugin:update       | Grants permission to modify a plug-in.                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:plugins:update</li> </ul>        |
| apig:plugin:bindApi      | Grants permission to bind a plug-in to APIs.                  | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:bindPlugins</li> </ul>      |

| Action                              | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                          |
|-------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|--------------------------------------------------------------------------------|
| apig:plugin:listUnbindApi           | Grants permission to query the APIs to which a plug-in can be bound.            | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:plugins:listUnbindApis</li> </ul>  |
| apig:plugin:listBoundApi            | Grants permission to query the APIs to which a plug-in has been bound.          | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:plugins:listBoundApis</li> </ul>   |
| apig:plugin:unbindApi               | Grants permission to unbind a plug-in from all APIs to which it has been bound. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:unbindPlugins</li> </ul>      |
| apig:apiGroup:listGatewayResponse   | Grants permission to query the responses of an API group.                       | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:list</li> </ul>   |
| apig:apiGroup:createGatewayResponse | Grants permission to create a response for an API group.                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:create</li> </ul> |
| apig:apiGroup:deleteGatewayResponse | Grants permission to delete a group response of an API group.                   | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:delete</li> </ul> |

| Action                                  | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                          |
|-----------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|--------------------------------------------------------------------------------|
| apig:apiGroup:getGatewayResponse        | Grants permission to query the details of a response defined for an API group.      | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:get</li> </ul>    |
| apig:apiGroup:updateGatewayResponse     | Grants permission to modify a response of an API group.                             | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:update</li> </ul> |
| apig:apiGroup:deleteGatewayResponseType | Grants permission to delete the response of an error type defined for an API group. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:update</li> </ul> |
| apig:apiGroup:getGatewayResponseType    | Grants permission to query the response of an error type defined for an API group.  | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:get</li> </ul>    |
| apig:apiGroup:updateGatewayResponseType | Grants permission to modify the response of an error type defined for an API group. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:gatewayResponses:update</li> </ul> |



| Action                            | Description                                                                                                                                                                | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                             |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------------------------------------------------------------------|
| apig:instance:listApiOutline      | Grants permission to query the number of APIs that have been published in the RELEASE environment and the number of APIs that have not been published in this environment. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:get</li> </ul>   |
| apig:instance:listAppOutline      | Grants permission to query the number of apps that have been authorized to access APIs and the number of apps that have not been authorized to access any APIs.            | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apps:get</li> </ul>   |
| apig:instance:listApiGroupOutline | Grants permission to query the number of API groups that have been listed on KooGallery and the number of API groups that have not been listed.                            | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:get</li> </ul> |

| Action                          | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                   |
|---------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------------------------------------------------------------------------|
| apig:environmentVariable:list   | Grants permission to query all environment variables under an API group. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:variables:list</li> </ul>   |
| apig:environmentVariable:create | Grants permission to create an environment variable.                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:variables:create</li> </ul> |
| apig:environmentVariable:delete | Grants permission to delete an environment variable.                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:variables:delete</li> </ul> |
| apig:environmentVariable:get    | Grants permission to query the details of an environment variable.       | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:variables:get</li> </ul>    |
| apig:environmentVariable:update | Grants permission to modify an environment variable.                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:variables:update</li> </ul> |
| apig:environment:list           | Grants permission to query environments.                                 | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:envs:list</li> </ul>        |
| apig:environment:create         | Grants permission to create an environment.                              | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:envs:create</li> </ul>      |
| apig:environment:delete         | Grants permission to delete an environment.                              | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:envs:delete</li> </ul>      |

| Action                               | Description                                                                                                         | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                 |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-----------------------------------------------------------------------|
| apig:environment:update              | Grants permission to modify the information about an environment.                                                   | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:envs:update</li> </ul>    |
| apig:instance:listMetricData         | Grants permission to query the monitoring metric data at a specified granularity in a specified period of time.     | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:metricData:get</li> </ul> |
| apig:instance:listApiMonitoring      | Grants permission to query the number of times APIs in an API group are called within a period.                     | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:get</li> </ul>       |
| apig:instance:listApiGroupMonitoring | Grants permission to query the total number of times all APIs in an API group are called based on the API group ID. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:groups:get</li> </ul>     |
| apig:requestThrottling:list          | Grants permission to query all the request throttling policies.                                                     | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:list</li> </ul> |

| Action                        | Description                                                                                                        | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                   |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------------------------------------------------------------------------|
| apig:requestThrottling:create | Grants permission to create a request throttling policy.                                                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:create</li> </ul> |
| apig:requestThrottling:delete | Grants permission to delete a request throttling policy and all binding relationships between the policy and APIs. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:delete</li> </ul> |
| apig:requestThrottling:get    | Grants permission to query the details of a request throttling policy.                                             | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:get</li> </ul>    |
| apig:requestThrottling:update | Grants permission to modify the information about a request throttling policy.                                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:update</li> </ul> |

| Action                             | Description                                                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                      |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------|
| apig:requestThrottling:batchDelete | Grants permission to delete multiple request throttling policies and all binding relationships between these policies and APIs. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:throttles:delete</li> </ul>    |
| apig:api:bindSignatureKey          | Grants permission to bind a signature key to one or more published APIs.                                                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:bindSigns</li> </ul>      |
| apig:api:unbindSignatureKey        | Grants permission to unbind a signature key from an API.                                                                        | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:unbindSigns</li> </ul>    |
| apig:signatureKey:listBoundApi     | Grants permission to query the APIs to which a signature key has been bound.                                                    | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:signs:listBoundApis</li> </ul> |
| apig:api:listBoundSignatureKey     | Grants permission to query the signature keys that have been bound to a specified API.                                          | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:apis:listBoundSigns</li> </ul> |

| Action                             | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                        |
|------------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------------|
| apig:signatureKey:listUnboundApis  | Grants permission to query the APIs to which a signature key has not been bound.       | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:signs:listUnboundApis</li> </ul> |
| apig:signatureKey:list             | Grants permission to query all the signature keys.                                     | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:signs:list</li> </ul>            |
| apig:signatureKey:create           | Grants permission to create a signature key.                                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:signs:create</li> </ul>          |
| apig:signatureKey:delete           | Grants permission to delete a signature key.                                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:signs:delete</li> </ul>          |
| apig:signatureKey:update           | Grants permission to modify the information about a signature key.                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:signs:update</li> </ul>          |
| apig:requestThrottling:listSpecial | Grants permission to query all excluded configurations of a request throttling policy. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:specialThrottles:get</li> </ul>  |

| Action                               | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                                                        |
|--------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| apig:requestThrottling:createSpecial | Grants permission to create an excluded configuration of a request throttling policy. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | <ul style="list-style-type: none"> <li>apig:specialThrottles:create</li> </ul>                               |
| apig:requestThrottling:deleteSpecial | Grants permission to delete an excluded configuration of a request throttling policy. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | <ul style="list-style-type: none"> <li>apig:specialThrottles:delete</li> </ul>                               |
| apig:requestThrottling:updateSpecial | Grants permission to modify an excluded configuration of a request throttling policy. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                  | <ul style="list-style-type: none"> <li>apig:specialThrottles:update</li> </ul>                               |
| apig:instance:listSingleInstanceTag  | Grants permission to query all tags of a gateway.                                     | List         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>apig:instanceTags:list</li> </ul>                                     |
| apig:instance:batchCreateOrDeleteTag | Grants permission to add tags to a gateway or delete the tags of a gateway.           | Write        | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>apig:instanceTags:create</li> <li>apig:instanceTags:delete</li> </ul> |
|                                      |                                                                                       |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              |                                                                                                              |

| Action                     | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                    |
|----------------------------|----------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| apig::listTag              | Grants permission to query all gateway tags of a project.      | List         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>apig:instanceTags:list</li> </ul> |
| apig:instance:getNumByTags | Grants permission to count dedicated gateways by tags.         | Read         | instance *                  | -                                                                                                                                              | -                                                                        |
|                            |                                                                |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                      |                                                                          |
| apig:instance:listByTags   | Grants permission to query dedicated gateways by tags.         | List         | instance *                  | -                                                                                                                                              | -                                                                        |
|                            |                                                                |              | -                           | <a href="#">g:TagKeys</a>                                                                                                                      |                                                                          |
| apig:instance:list         | Grants permission to query dedicated gateways.                 | List         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>apig:instances:list</li> </ul>    |
| apig:instance:create       | Grants permission to create a dedicated gateway.               | Write        | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              | <ul style="list-style-type: none"> <li>apig:instances:create</li> </ul>  |
| apig:instance:delete       | Grants permission to delete a dedicated gateway.               | Write        | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>apig:instances:delete</li> </ul>  |
| apig:instance:get          | Grants permission to query the details of a dedicated gateway. | Read         | instance *                  | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>apig:instances:get</li> </ul>     |



| Action                                   | Description                                                                                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| apig:instance:update                     | Grants permission to update a dedicated gateway.                                                        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:unbindEip                  | Grants permission to unbind the EIP of a dedicated gateway.                                             | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:bindOrChangeEip            | Grants permission to bind an EIP to a dedicated gateway or update the EIP bound to a dedicated gateway. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:deleteOutboundEip          | Grants permission to disable public access for a dedicated gateway.                                     | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:createOutboundEip          | Grants permission to enable public access for a dedicated gateway.                                      | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:changeOutboundEipBandwidth | Grants permission to update the outbound access bandwidth of a dedicated gateway.                       | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |

| Action                                  | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                   |
|-----------------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| apig:instance:getCreateProgress         | Grants permission to query the creation progress of a dedicated gateway.               | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                       |
| apig:instance:deleteIngressEip          | Grants permission to disable inbound access for a dedicated gateway.                   | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:createIngressEip          | Grants permission to enable inbound access for a dedicated gateway.                    | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:changeIngressEipBandwidth | Grants permission to update the inbound access bandwidth of a dedicated gateway.       | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:update |
| apig:instance:resize                    | Grants permission to create a flavor change order for a pay-per-use dedicated gateway. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                       |

| Action                               | Description                                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                  |
|--------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| apig:instance:getInstanceRestriction | Grants permission to query the constraint of a gateway.               | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:instances:get   |
| apig:instance:listParameters         | Grants permission to query the features of a gateway.                 | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:features:list   |
| apig:instance:updateParameter        | Grants permission to configure a feature for a gateway.               | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • apig:features:create |
| apig:instance:listFeatures           | Grants permission to the features supported by the dedicated gateway. | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                      |
| apig:instance:importMicroservice     | Grants permission to import a microservice.                           | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | • apig:apis:import     |
| apig:apiGroup:bindDomain             | Grants permission to binding a custom domain name from an API group.  | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | • apig:domains:create  |

| Action                                             | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                            |
|----------------------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------------|
| apig:apiGroup:unbindDomain                         | Grants permission to unbind a custom domain name from an API group.                   | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:delete</li> </ul>            |
| apig:apiGroup:updateDomainConfig                   | Grants permission to modify the configuration of a domain name bound to an API group. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:update</li> </ul>            |
| apig:apiGroup:createAndBindCertificateToDomain     | Grants permission to add a certificate to a specific domain name.                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:bindCertificate</li> </ul>   |
| apig:apiGroup:unbindAndDeleteCertificateFromDomain | Grants permission to delete a certificate that is no longer needed or has expired.    | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:unbindCertificate</li> </ul> |
| apig:apiGroup:getCertificateOfDomain               | Grants permission to query the details of the certificate bound to a domain name.     | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:getCertificate</li> </ul>    |

| Action                              | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                |
|-------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| apig:apiGroup:updateSLDomainSetting | Grants permission to set whether the second-level domain can be accessed. | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:domains:updateSLDomainSetting</li> </ul> |
| apig:customAuthorizer:list          | Grants permission to query all the custom authorizers under a gateway.    | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:authorizers:list</li> </ul>              |
| apig:customAuthorizer:create        | Grants permission to create a custom authorizer.                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:authorizers:create</li> </ul>            |
| apig:customAuthorizer:delete        | Grants permission to delete a custom authorizer.                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:authorizers:delete</li> </ul>            |
| apig:customAuthorizer:get           | Grants permission to query the details of a custom authorizer.            | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:authorizers:get</li> </ul>               |
| apig:customAuthorizer:update        | Grants permission to modify a custom authorizer.                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>apig:authorizers:update</li> </ul>            |

| Action                                            | Description                                                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| apig:instance:listVpcEndpoint                     | Grants permission to query connections of a dedicated gateway VPC endpoint service.                | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| apig:instance:acceptOrRejectVpcEndpointConnection | Grants permission to accept or reject a dedicated gateway VPC endpoint for a VPC endpoint service. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| apig:instance:listVpcEndpointPermission           | Grants permission to query the whitelist records of a dedicated gateway VPC endpoint service.      | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| apig:instance:batchAddVpcEndpointPermission       | Grants permission to batch add whitelist records of a dedicated gateway VPC endpoint service.      | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                         | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                                                           |
|------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| apig:instance:batchDeleteVpcEndpointPermission | Grants permission to batch delete whitelist records of a dedicated gateway VPC endpoint service. | Write        | instance *                  | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -                                                               |
| apig:app:deleteAcl                             | Grants permission to delete access control for a client configuration.                           | Write        | instance *                  | g:ResourceTag/<tag-key>                                                                                        | <ul style="list-style-type: none"> <li>apig:apps:get</li> </ul> |
| apig:app:getAcl                                | Grants permission to query the details about the app access control.                             | Read         | instance *                  | g:ResourceTag/<tag-key>                                                                                        | <ul style="list-style-type: none"> <li>apig:apps:get</li> </ul> |
| apig:app:updateAcl                             | Grants permission to configure access control for a client configuration.                        | Write        | instance *                  | g:ResourceTag/<tag-key>                                                                                        | <ul style="list-style-type: none"> <li>apig:apps:get</li> </ul> |
| apig:clientQuota:list                          | Grants permission to query client quotas.                                                        | List         | instance *                  | g:ResourceTag/<tag-key>                                                                                        | -                                                               |
| apig:clientQuota:create                        | Grants permission to create a client quota.                                                      | Write        | instance *                  | g:ResourceTag/<tag-key>                                                                                        | -                                                               |
| apig:clientQuota:delete                        | Grants permission to delete a client quota.                                                      | Write        | instance *                  | g:ResourceTag/<tag-key>                                                                                        | -                                                               |

| Action                           | Description                                                                                          | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|----------------------------------|------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| apig:clientQuota:get             | Grants permission to querying the details of a client quota.                                         | Read         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| apig:clientQuota:update          | Grants permission to modify a client quota.                                                          | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| apig:clientQuota:listBoundApp    | Grants permission to query client applications bound to a client quota.                              | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| apig:clientQuota:bindApp         | Grants permission to bind client applications to a client quota.                                     | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| apig:clientQuota:unbindApp       | Grants permission to unbind client applications from a client quota.                                 | Write        | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| apig:clientQuota:listUnboundApp  | Grants permission to query client applications that are available for being bound to a client quota. | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| apig:instance:listFeatureHistory | Grants permission to query the history list of feature                                               | List         | instance *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |



| Action                                    | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| apig:instance:addCustomIngressPort        | Grants permission to add customized ingress ports of the instance.        | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| apig:instance:listCustomIngressPort       | Grants permission to query customized ingress ports of the instance.      | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| apig:instance:deleteCustomIngressPort     | Grants permission to delete customized ingress ports of the instance.     | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| apig:instance:listCustomIngressPortDomain | Grants permission to query the domains info of a customized ingress port. | List         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

Each API of apig usually supports one or more actions. [Table 3-216](#) lists the supported actions and dependencies.

**Table 3-216** Actions and dependencies supported by apig APIs

| API                                                  | Action        | Dependencies      |
|------------------------------------------------------|---------------|-------------------|
| GET /{project_id}/apigw/instances/{instance_id}/acls | apig:acl:list | apig:instance:get |

| API                                                                               | Action                  | Dependencies                                                                                                    |
|-----------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------|
| POST /{project_id}/apigw/instances/{instance_id}/acls                             | apig:acl:create         | apig:instance:get                                                                                               |
| PUT /{project_id}/apigw/instances/{instance_id}/acls                              | apig:acl:batchDelete    | apig:instance:get                                                                                               |
| DELETE /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}                  | apig:acl:delete         | apig:instance:get                                                                                               |
| GET /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}                     | apig:acl:get            | apig:instance:get                                                                                               |
| PUT /{project_id}/apigw/instances/{instance_id}/acls/{acl_id}                     | apig:acl:update         | apig:instance:get                                                                                               |
| POST /{project_id}/apigw/instances/{instance_id}/acl-bindings                     | apig:api:bindAcl        | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:acl:get</li> </ul> |
| PUT /{project_id}/apigw/instances/{instance_id}/acl-bindings                      | apig:api:batchUnbindAcl | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:acl:get</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/acl-bindings/{acl_bindings_id} | apig:api:unbindAcl      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:acl:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-acls          | apig:api:listBoundAcl   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-apis          | apig:acl:listBoundApi   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:acl:get</li> </ul>                       |

| API                                                                                        | Action                                | Dependencies                                                                                                                  |
|--------------------------------------------------------------------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/unbound-apis                  | apig:acl:listUnboundApi               | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:acl:get</li> </ul>                                     |
| POST /{project_id}/apigw/instances/{instance_id}/throttle-bindings                         | apig:api:bindRequestThrottling        | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:requestThrottling:get</li> </ul> |
| PUT /{project_id}/apigw/instances/{instance_id}/throttle-bindings                          | apig:api:batchUnbindRequestThrottling | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:requestThrottling:get</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/throttle-bindings/{throttle_binding_id} | apig:api:unbindRequestThrottling      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:requestThrottling:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-apis              | apig:requestThrottling:listBoundApi   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:requestThrottling:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-throttles         | apig:api:listBoundRequestThrottling   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> </ul>                                     |
| GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/unbound-apis             | apig:requestThrottling:listUnboundApi | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:requestThrottling:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/api-groups                                 | apig:apiGroup:list                    | apig:instance:get                                                                                                             |
| POST /{project_id}/apigw/instances/{instance_id}/api-groups                                | apig:apiGroup:create                  | apig:instance:get                                                                                                             |

| API                                                                                      | Action                                        | Dependencies                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/api-<br>groups/{group_id} | apig:apiGroup:delete                          | apig:instance:get                                                                                                                                                                                                                                  |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/api-<br>groups/{group_id}        | apig:apiGroup:get                             | apig:instance:get                                                                                                                                                                                                                                  |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/api-<br>groups/{group_id}        | apig:apiGroup:update                          | apig:instance:get                                                                                                                                                                                                                                  |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/api-<br>groups/check            | apig:apiGroup:checkApiGro<br>upNameExistOrNot | apig:instance:get                                                                                                                                                                                                                                  |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/apis                             | apig:api:list                                 | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                                                                                                                                 |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/apis                            | apig:api:create                               | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> <li>• apig:loadBalanceChan-<br/>nel:get</li> <li>• apig:customAuthorizer:g<br/>et</li> <li>• functiongraph:function:g<br/>etFunctionConfig</li> </ul> |
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/apis/<br>{api_id}         | apig:api:delete                               | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                                                                                                                                 |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/apis/<br>{api_id}                | apig:api:get                                  | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                                                                                                                                 |

| API                                                                           | Action                                   | Dependencies                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}                 | apig:api:update                          | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:loadBalanceChannel:get</li> <li>apig:customAuthorizer:get</li> <li>functiongraph:function:getFunctionConfig</li> </ul> |
| POST /{project_id}/apigw/instances/{instance_id}/apis/action                  | apig:api:onlineOrOffline                 | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:environment:list</li> </ul>                                                                                            |
| POST /{project_id}/apigw/instances/{instance_id}/apis/check                   | apig:api:checkApiPathOrApiNameExistOrNot | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                                                                                                                           |
| POST /{project_id}/apigw/instances/{instance_id}/apis/debug/{api_id}          | apig:api:debug                           | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                                                                                                                           |
| POST /{project_id}/apigw/instances/{instance_id}/apis/publish                 | apig:api:batchOnlineOrOffline            | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:environment:list</li> </ul>                                                                                            |
| GET /{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}         | apig:api:listHistoryVersion              | apig:instance:get                                                                                                                                                                                                        |
| PUT /{project_id}/apigw/instances/{instance_id}/apis/publish/{api_id}         | apig:api:switchVersion                   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> </ul>                                                                                                                                |
| GET /{project_id}/apigw/instances/{instance_id}/apis/runtime/{api_id}         | apig:api:getRuntimeDefinition            | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:environment:list</li> </ul>                                                                                                                       |
| DELETE /{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id} | apig:api:deleteHistoryVersion            | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:environment:list</li> </ul>                                                                                            |

| API                                                                                      | Action                     | Dependencies                                                                                  |
|------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}               | apig:api:getHistoryVersion | apig:instance:get                                                                             |
| GET /{project_id}/apigw/instances/{instance_id}/apps                                     | apig:app:list              | apig:instance:get                                                                             |
| POST /{project_id}/apigw/instances/{instance_id}/apps                                    | apig:app:create            | apig:instance:get                                                                             |
| DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}                         | apig:app:delete            | apig:instance:get                                                                             |
| GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}                            | apig:app:get               | apig:instance:get                                                                             |
| PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}                            | apig:app:update            | apig:instance:get                                                                             |
| GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes                  | apig:app:listAppCode       | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:app:get</li> </ul> |
| POST /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes                 | apig:app:createAppCode     | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:app:get</li> </ul> |
| PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes                  | apig:app:generateAppCode   | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:app:get</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id} | apig:app:deleteAppCode     | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:app:get</li> </ul> |

| API                                                                                   | Action                  | Dependencies                                                                                                    |
|---------------------------------------------------------------------------------------|-------------------------|-----------------------------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id} | apig:app:getAppCode     | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul>                       |
| PUT /{project_id}/apigw/instances/{instance_id}/apps/secret/{app_id}                  | apig:app:resetSecret    | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/apps/validation/{app_id}              | apig:app:validate       | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/bound-quota             | apig:app:getBoundQuota  | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul>                       |
| POST /{project_id}/apigw/instances/{instance_id}/app-auths                            | apig:app:bindApi        | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> <li>apig:api:get</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/app-auths/{app_auth_id}            | apig:app:unbindApi      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> <li>apig:api:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apis                 | apig:app:listBoundApi   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apps                 | apig:api:listBoundApp   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/app-auths/unbinded-apis               | apig:app:listUnboundApi | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul>                       |

| API                                                                               | Action          | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>openapi/export       | apig:api:export | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:api:list</li> <li>• apig:api:get</li> <li>• apig:api:listBoundAcl</li> <li>• apig:acl:get</li> <li>• apig:api:listBoundRequestThrottling</li> <li>• apig:requestThrottling:get</li> <li>• apig:apiGroup:get</li> <li>• apig:apiGroup:getGatewayResponse</li> <li>• apig:environment:list</li> <li>• apig:api:listBoundPlugin</li> <li>• apig:plugin:get</li> </ul> |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>openapi/async-export | apig:api:export | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:api:list</li> <li>• apig:api:get</li> <li>• apig:api:listBoundAcl</li> <li>• apig:acl:get</li> <li>• apig:api:listBoundRequestThrottling</li> <li>• apig:requestThrottling:get</li> <li>• apig:apiGroup:get</li> <li>• apig:apiGroup:getGatewayResponse</li> <li>• apig:environment:list</li> <li>• apig:api:listBoundPlugin</li> <li>• apig:plugin:get</li> </ul> |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>openapi/import       | apig:api:import | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:api:get</li> <li>• apig:acl:get</li> <li>• apig:requestThrottling:get</li> <li>• apig:apiGroup:get</li> <li>• apig:apiGroup:getGatewayResponse</li> <li>• apig:environment:list</li> <li>• apig:plugin:get</li> </ul>                                                                                                                                              |



| API                                                                    | Action                             | Dependencies                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /{project_id}/apigw/instances/{instance_id}/openapi/async-import  | apig:api:import                    | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:api:get</li> <li>• apig:acl:get</li> <li>• apig:requestThrottling:get</li> <li>• apig:apiGroup:get</li> <li>• apig:apiGroup:getGatewayResponse</li> <li>• apig:environment:list</li> <li>• apig:plugin:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/async-tasks/{task_id}  | apig:asyncTask:get                 | apig:instance:get                                                                                                                                                                                                                                                                                |
| GET /{project_id}/apigw/certificates                                   | apig:certificate:list              | -                                                                                                                                                                                                                                                                                                |
| POST /{project_id}/apigw/certificates                                  | apig:certificate:create            | apig:instance:get                                                                                                                                                                                                                                                                                |
| DELETE /{project_id}/apigw/certificates/{certificate_id}               | apig:certificate:delete            | -                                                                                                                                                                                                                                                                                                |
| GET /{project_id}/apigw/certificates/{certificate_id}                  | apig:certificate:get               | -                                                                                                                                                                                                                                                                                                |
| PUT /{project_id}/apigw/certificates/{certificate_id}                  | apig:certificate:update            | apig:instance:get                                                                                                                                                                                                                                                                                |
| GET /{project_id}/apigw/certificates/{certificate_id}/attached-domains | apig:certificate:listBoundDomain   | -                                                                                                                                                                                                                                                                                                |
| POST /{project_id}/apigw/certificates/{certificate_id}/domains/attach  | apig:certificate:batchBindDomain   | <ul style="list-style-type: none"> <li>• apig:certificate:get</li> <li>• apig:apiGroup:get</li> </ul>                                                                                                                                                                                            |
| POST /{project_id}/apigw/certificates/{certificate_id}/domains/detach  | apig:certificate:batchUnbindDomain | <ul style="list-style-type: none"> <li>• apig:certificate:get</li> <li>• apig:apiGroup:get</li> </ul>                                                                                                                                                                                            |

| API                                                                                                            | Action                                         | Dependencies                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/attach | apig:apiGroup:batchBindCertificateToDomain     | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> <li>• apig:certificate:get</li> </ul>                                                             |
| POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/detach | apig:apiGroup:batchUnbindCertificateFromDomain | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> <li>• apig:certificate:get</li> </ul>                                                             |
| GET /{project_id}/apigw/instances/{instance_id}/vpc-channels                                                   | apig:loadBalanceChannel:list                   | apig:instance:get                                                                                                                                                                              |
| POST /{project_id}/apigw/instances/{instance_id}/vpc-channels                                                  | apig:loadBalanceChannel:create                 | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• cce:cluster:getCluster</li> <li>• ecs:cloudServers:showServer</li> <li>• cce:cluster:generateClientCredential</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}                               | apig:loadBalanceChannel:delete                 | apig:instance:get                                                                                                                                                                              |
| GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}                                  | apig:loadBalanceChannel:get                    | apig:instance:get                                                                                                                                                                              |
| PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}                                  | apig:loadBalanceChannel:update                 | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• cce:cluster:getCluster</li> <li>• ecs:cloudServers:showServer</li> <li>• cce:cluster:generateClientCredential</li> </ul> |

| API                                                                                                              | Action                                           | Dependencies                                                                                                 |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/health-config                      | apig:loadBalanceChannel:updateHealthCheck-Config | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:loadBalanceChannel:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups                      | apig:loadBalanceChannel:listServerGroup          | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:loadBalanceChannel:get</li> </ul> |
| POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups                     | apig:loadBalanceChannel:createServerGroup        | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:loadBalanceChannel:get</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id} | apig:loadBalanceChannel:deleteServerGroup        | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:loadBalanceChannel:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}    | apig:loadBalanceChannel:getServerGroup           | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:loadBalanceChannel:get</li> </ul> |
| PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}    | apig:loadBalanceChannel:updateServerGroup        | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:loadBalanceChannel:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members                            | apig:loadBalanceChannel:listBackendServerAddress | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:loadBalanceChannel:get</li> </ul> |

| API                                                                                                  | Action                                                   | Dependencies                                                                                                                                  |
|------------------------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members               | apig:loadBalanceChannel:createBackendServerAddress       | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:loadBalanceChannel:get</li> <li>ecs:cloudServers:showServer</li> </ul> |
| PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members                | apig:loadBalanceChannel:updateBackendServerAddress       | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:loadBalanceChannel:get</li> <li>ecs:cloudServers:showServer</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/{member_id} | apig:loadBalanceChannel:deleteBackendServerAddress       | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:loadBalanceChannel:get</li> </ul>                                      |
| POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-disable | apig:loadBalanceChannel:batchDisableBackendServerAddress | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:loadBalanceChannel:get</li> </ul>                                      |
| POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-enable  | apig:loadBalanceChannel:batchEnableBackendServerAddress  | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:loadBalanceChannel:get</li> </ul>                                      |
| GET /{project_id}/apigw/instances/{instance_id}/tags                                                 | apig:instance:listTag                                    | apig:instance:get                                                                                                                             |
| GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attachable-plugins                     | apig:api:listUnboundPlugin                               | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> </ul>                                                     |

| API                                                                            | Action                   | Dependencies                                                                                                                                               |
|--------------------------------------------------------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attached-plugins | apig:api:listBoundPlugin | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> </ul>                                                                  |
| POST /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/attach  | apig:api:bindPlugin      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:plugin:get</li> </ul>                                         |
| PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/detach   | apig:api:unbindPlugin    | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:plugin:get</li> </ul>                                         |
| GET /{project_id}/apigw/instances/{instance_id}/plugins                        | apig:plugin:list         | apig:instance:get                                                                                                                                          |
| POST /{project_id}/apigw/instances/{instance_id}/plugins                       | apig:plugin:create       | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:loadBalanceChannel:get</li> <li>functiongraph:function:getFunctionConfig</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}         | apig:plugin:delete       | apig:instance:get                                                                                                                                          |
| GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}            | apig:plugin:get          | apig:instance:get                                                                                                                                          |
| PUT /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}            | apig:plugin:update       | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:loadBalanceChannel:get</li> <li>functiongraph:function:getFunctionConfig</li> </ul> |
| POST /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attach    | apig:plugin:bindApi      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:plugin:get</li> </ul>                                         |

| API                                                                                                      | Action                              | Dependencies                                                                                                       |
|----------------------------------------------------------------------------------------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attachable-apis                      | apig:plugin:listUnbindApi           | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:plugin:get</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attached-apis                        | apig:plugin:listBoundApi            | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:plugin:get</li> </ul>                       |
| PUT /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/detach                               | apig:plugin:unbindApi               | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:plugin:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses                  | apig:apiGroup:listGatewayResponse   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                     |
| POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses                 | apig:apiGroup:createGatewayResponse | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                     |
| DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id} | apig:apiGroup:deleteGatewayResponse | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                     |
| GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}    | apig:apiGroup:getGatewayResponse    | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                     |
| PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}    | apig:apiGroup:updateGatewayResponse | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                     |

| API                                                                                                                                                  | Action                                  | Dependencies                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/api-<br>groups/{group_id}/<br>gateway-responses/<br>{response_id}/<br>{response_type} | apig:apiGroup:deleteGatewayResponseType | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                  |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/api-<br>groups/{group_id}/<br>gateway-responses/<br>{response_id}/<br>{response_type}        | apig:apiGroup:getGatewayResponseType    | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                  |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/api-<br>groups/{group_id}/<br>gateway-responses/<br>{response_id}/<br>{response_type}        | apig:apiGroup:updateGatewayResponseType | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                  |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>resources/outline/<br>apis                                                               | apig:instance:listApiOutline            | apig:instance:get                                                                                                                   |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>resources/outline/<br>apps                                                               | apig:instance:listAppOutline            | apig:instance:get                                                                                                                   |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>resources/outline/<br>groups                                                             | apig:instance:listApiGroupOutline       | apig:instance:get                                                                                                                   |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/env-<br>variables                                                                            | apig:environmentVariable:list           | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> <li>• apig:environment:list</li> </ul> |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/env-<br>variables                                                                           | apig:environmentVariable:create         | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> <li>• apig:environment:list</li> </ul> |

| API                                                                                                    | Action                               | Dependencies                                                                                                                  |
|--------------------------------------------------------------------------------------------------------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/env-<br>variables/<br>{env_variable_id} | apig:environmentVariable:delete      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:environment:list</li> </ul> |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/env-<br>variables/<br>{env_variable_id}        | apig:environmentVariable:get         | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:environment:list</li> </ul> |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/env-<br>variables/<br>{env_variable_id}        | apig:environmentVariable:update      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:environment:list</li> </ul> |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/envs                                           | apig:environment:list                | apig:instance:get                                                                                                             |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/envs                                          | apig:environment:create              | apig:instance:get                                                                                                             |
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/envs/<br>{env_id}                       | apig:environment:delete              | apig:instance:get                                                                                                             |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/envs/<br>{env_id}                              | apig:environment:update              | apig:instance:get                                                                                                             |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>metric-data                                | apig:instance:listMetricData         | apig:instance:get                                                                                                             |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>statistics/api/latest                      | apig:instance:listApiMonitoring      | apig:instance:get                                                                                                             |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>statistics/group/<br>latest                | apig:instance:listApiGroupMonitoring | apig:instance:get                                                                                                             |



| API                                                                                 | Action                         | Dependencies                                                                                                              |
|-------------------------------------------------------------------------------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/throttles                           | apig:requestThrottling:list    | apig:instance:get                                                                                                         |
| POST /{project_id}/apigw/instances/{instance_id}/throttles                          | apig:requestThrottling:create  | apig:instance:get                                                                                                         |
| DELETE /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}          | apig:requestThrottling:delete  | apig:instance:get                                                                                                         |
| GET /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}             | apig:requestThrottling:get     | apig:instance:get                                                                                                         |
| PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}             | apig:requestThrottling:update  | apig:instance:get                                                                                                         |
| POST /{project_id}/apigw/instances/{instance_id}/sign-bindings                      | apig:api:bindSignatureKey      | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:signatureKey:list</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/sign-bindings/{sign_bindings_id} | apig:api:unbindSignatureKey    | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> <li>apig:signatureKey:list</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-apis           | apig:signatureKey:listBoundApi | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:signatureKey:list</li> </ul>                       |
| GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-signs          | apig:api:listBoundSignatureKey | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:api:get</li> </ul>                                 |

| API                                                                                                        | Action                               | Dependencies                                                                                            |
|------------------------------------------------------------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/unbound-apis                                 | apig:signatureKey:listUnboundApi     | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:signatureKey:list</li> </ul>     |
| GET /{project_id}/apigw/instances/{instance_id}/signs                                                      | apig:signatureKey:list               | apig:instance:get                                                                                       |
| POST /{project_id}/apigw/instances/{instance_id}/signs                                                     | apig:signatureKey:create             | apig:instance:get                                                                                       |
| DELETE /{project_id}/apigw/instances/{instance_id}/signs/{sign_id}                                         | apig:signatureKey:delete             | apig:instance:get                                                                                       |
| PUT /{project_id}/apigw/instances/{instance_id}/signs/{sign_id}                                            | apig:signatureKey:update             | apig:instance:get                                                                                       |
| GET /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials                  | apig:requestThrottling:listSpecial   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:requestThrottling:get</li> </ul> |
| POST /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials                 | apig:requestThrottling:createSpecial | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:requestThrottling:get</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id} | apig:requestThrottling:deleteSpecial | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:requestThrottling:get</li> </ul> |

| API                                                                                                     | Action                               | Dependencies                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id} | apig:requestThrottling:updateSpecial | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:requestThrottling:get</li> </ul>                                                                                                                    |
| GET /{project_id}/apigw/instances/{instance_id}/instance-tags                                           | apig:instance:listSingleInstanceTag  | apig:instance:get                                                                                                                                                                                                          |
| POST /{project_id}/apigw/instances/{instance_id}/instance-tags/action                                   | apig:instance:batchCreateOrDeleteTag | apig:instance:get                                                                                                                                                                                                          |
| GET /{project_id}/apigw/instance-tags                                                                   | apig::listTag                        | apig:instance:get                                                                                                                                                                                                          |
| POST /{project_id}/apigw/resource-instances/count                                                       | apig:instance:getNumByTags           | -                                                                                                                                                                                                                          |
| POST /{project_id}/apigw/resource-instances/filter                                                      | apig:instance:listByTags             | -                                                                                                                                                                                                                          |
| GET /{project_id}/apigw/instances                                                                       | apig:instance:list                   | -                                                                                                                                                                                                                          |
| POST /{project_id}/apigw/instances                                                                      | apig:instance:create                 | <ul style="list-style-type: none"> <li>vpc:securityGroups:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>eip:publicIps:get</li> <li>eip:publicIps:update</li> <li>eps:enterpriseProjects:list</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}                                                      | apig:instance:delete                 | <ul style="list-style-type: none"> <li>eip:publicIps:get</li> <li>eip:publicIps:update</li> <li>vpc:ports:delete</li> </ul>                                                                                                |
| GET /{project_id}/apigw/instances/{instance_id}                                                         | apig:instance:get                    | -                                                                                                                                                                                                                          |
| PUT /{project_id}/apigw/instances/{instance_id}                                                         | apig:instance:update                 | <ul style="list-style-type: none"> <li>vpc:securityGroups:get</li> <li>vpc:ports:update</li> </ul>                                                                                                                         |

| API                                                                            | Action                                   | Dependencies                                                                                      |
|--------------------------------------------------------------------------------|------------------------------------------|---------------------------------------------------------------------------------------------------|
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/eip             | apig:instance:unbindEip                  | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>eip:publicIps:update</li> </ul> |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/eip                    | apig:instance:bindOrChangeEip            | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>eip:publicIps:update</li> </ul> |
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/nat-<br>eip     | apig:instance:deleteOutboundEip          | apig:instance:get                                                                                 |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/nat-<br>eip           | apig:instance:createOutboundEip          | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>vpc:ports:get</li> </ul>        |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/nat-<br>eip            | apig:instance:changeOutboundEipBandwidth | apig:instance:get                                                                                 |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>progress           | apig:instance:getCreateProgress          | -                                                                                                 |
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/<br>ingress-eip | apig:instance:deleteIngressEip           | apig:instance:get                                                                                 |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>ingress-eip       | apig:instance:createIngressEip           | apig:instance:get                                                                                 |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>ingress-eip        | apig:instance:changeIngressEipBandwidth  | apig:instance:get                                                                                 |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>postpaid-resize   | apig:instance:resize                     | apig:instance:get                                                                                 |

| API                                                                                          | Action                           | Dependencies                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /{project_id}/apigw/instances/{instance_id}/restriction                                  | apig:instance:getRestriction     | apig:instance:get                                                                                                                                                                                                                                                                                                                |
| GET /{project_id}/apigw/instances/{instance_id}/features                                     | apig:instance:listParameter      | apig:instance:get                                                                                                                                                                                                                                                                                                                |
| POST /{project_id}/apigw/instances/{instance_id}/features                                    | apig:instance:updateParameter    | apig:instance:get                                                                                                                                                                                                                                                                                                                |
| GET /{project_id}/apigw/instances/{instance_id}/instance-features                            | apig:instance:listFeature        | apig:instance:get                                                                                                                                                                                                                                                                                                                |
| POST /{project_id}/apigw/instances/{instance_id}/microservice/import                         | apig:instance:importMicroservice | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:api:create</li> <li>• apig:apiGroup:get</li> <li>• apig:apiGroup:create</li> <li>• apig:loadBalanceChannel:get</li> <li>• apig:loadBalanceChannel:create</li> <li>• cce:cluster:getCluster</li> <li>• cce:cluster:generateClientCredential</li> </ul> |
| POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains               | apig:apiGroup:bindDomain         | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                                                                                                                                                                                                               |
| DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id} | apig:apiGroup:unbindDomain       | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• apig:apiGroup:get</li> </ul>                                                                                                                                                                                                                               |

| API                                                                                                                       | Action                                             | Dependencies                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}                                 | apig:apiGroup:updateDomainConfig                   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                               |
| POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate                    | apig:apiGroup:createAndBindCertificateToDomain     | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:certificate:get</li> </ul> |
| DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id} | apig:apiGroup:unbindAndDeleteCertificateFromDomain | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:certificate:get</li> </ul> |
| GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}    | apig:apiGroup:getCertificateOfDomain               | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:certificate:get</li> </ul> |
| PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/sl-domain-access-settings                           | apig:apiGroup:updateSLDomainSetting                | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> </ul>                               |
| GET /{project_id}/apigw/instances/{instance_id}/authorizers                                                               | apig:customAuthorizer:list                         | apig:instance:get                                                                                                            |
| POST /{project_id}/apigw/instances/{instance_id}/authorizers                                                              | apig:customAuthorizer:create                       | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>functiongraph:function:getFunctionConfig</li> </ul>        |

| API                                                                                                        | Action                                            | Dependencies                                                                                                              |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/<br>authorizers/<br>{authorizer_id}         | apig:customAuthorizer:delete                      | apig:instance:get                                                                                                         |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>authorizers/<br>{authorizer_id}                | apig:customAuthorizer:get                         | apig:instance:get                                                                                                         |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/<br>authorizers/<br>{authorizer_id}                | apig:customAuthorizer:update                      | <ul style="list-style-type: none"> <li>• apig:instance:get</li> <li>• functiongraph:function:getFunctionConfig</li> </ul> |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/vpc-<br>endpoint/<br>connections                   | apig:instance:listVpcEndpoint                     | apig:instance:get                                                                                                         |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/vpc-<br>endpoint/<br>connections/action           | apig:instance:acceptOrRejectVpcEndpointConnection | apig:instance:get                                                                                                         |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/vpc-<br>endpoint/<br>permissions                   | apig:instance:listVpcEndpointPermission           | apig:instance:get                                                                                                         |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/vpc-<br>endpoint/<br>permissions/batch-<br>add    | apig:instance:batchAddVpcEndpointPermission       | apig:instance:get                                                                                                         |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/vpc-<br>endpoint/<br>permissions/batch-<br>delete | apig:instance:batchDeleteVpcEndpointPermission    | apig:instance:get                                                                                                         |

| API                                                                                                      | Action                            | Dependencies                                                                              |
|----------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------------------------------|
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/apps/<br>{app_id}/app-acl                 | apig:app:deleteAcl                | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul> |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/apps/<br>{app_id}/app-acl                        | apig:app:getAcl                   | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul> |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/apps/<br>{app_id}/app-acl                        | apig:app:updateAcl                | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> </ul> |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/app-<br>quotas                                   | apig:clientQuota:list             | apig:instance:get                                                                         |
| POST /{project_id}/<br>apigw/instances/<br>{instance_id}/app-<br>quotas                                  | apig:clientQuota:create           | apig:instance:get                                                                         |
| DELETE /<br>{project_id}/apigw/<br>instances/<br>{instance_id}/app-<br>quotas/<br>{app_quota_id}         | apig:clientQuota:delete           | apig:instance:get                                                                         |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/app-<br>quotas/<br>{app_quota_id}                | apig:clientQuota:get              | apig:instance:get                                                                         |
| PUT /{project_id}/<br>apigw/instances/<br>{instance_id}/app-<br>quotas/<br>{app_quota_id}                | apig:clientQuota:update           | apig:instance:get                                                                         |
| GET /{project_id}/<br>apigw/instances/<br>{instance_id}/app-<br>quotas/<br>{app_quota_id}/<br>bound-apps | apig:clientQuota:listBoundA<br>pp | apig:instance:get                                                                         |



| API                                                                                              | Action                                    | Dependencies                                                                                                                                |
|--------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| POST /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/binding-apps          | apig:clientQuota:bindApp                  | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:clientQuota:get</li> </ul>                                           |
| DELETE /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps/{app_id} | apig:clientQuota:unbindApp                | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:app:get</li> <li>apig:clientQuota:get</li> </ul>                     |
| GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bindable-apps          | apig:clientQuota:listUnboundApp           | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:clientQuota:get</li> </ul>                                           |
| POST /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports                            | apig:instance:addCustomIngressPort        | apig:instance:get                                                                                                                           |
| GET /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports                             | apig:instance:listCustomIngressPort       | apig:instance:get                                                                                                                           |
| DELETE /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}        | apig:instance:deleteCustomIngressPort     | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:instance:listCustomIngressPort</li> </ul>                            |
| GET /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}/domains   | apig:instance:listCustomIngressPortDomain | <ul style="list-style-type: none"> <li>apig:instance:get</li> <li>apig:apiGroup:get</li> <li>apig:instance:listCustomIngressPort</li> </ul> |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-217](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for apig.

**Table 3-217** Resource types supported by apig

| Resource Type | URN                                               |
|---------------|---------------------------------------------------|
| instance      | apig:<region>:<account-id>:instance:<instance-id> |

## Conditions

apig does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.10.6 Distributed Cache Service (DCS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DCS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DCS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DCS.

**Table 3-218** Actions supported by DCS

| Action                      | Description                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                       | Alias             |
|-----------------------------|--------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| dcs:instance:create         | Grants permission to create DCS instances.                         | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">dcs:backupEnabled</a></li> </ul> | -                 |
| dcs:instance:list           | Grants permission to query the DCS instance list.                  | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                               | -                 |
| dcs:instance:exportListFile | Grants permission to download the exported DCS instance list file. | List         | -                           | -                                                                                                                                                                                                                                   | dcs:instance:list |
| dcs:instance:delete         | Grants permission to delete DCS instances.                         | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                               | -                 |
| dcs:instance:get            | Grants permission to query DCS instances.                          | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                               | -                 |
| dcs:instance:modify         | Grants permission to modify DCS instances.                         | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">dcs:backupEnabled</a></li> </ul>                                                                                              | -                 |
| dcs:instance:scale          | Grants permission to scale up DCS instances.                       | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                               | -                 |

| Action                           | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                         | Alias                           |
|----------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------|
| dc:instance:sw                   | Grants permission to perform master/replica switchover on DCS instances. | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                               |
| dc:instance:modifyAuthInfo       | Grants permission to modify the passwords of DCS instances.              | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:resetAuthInfo       |
| dc:instance:modifyStatus         | Grants permission to restart DCS instances or clear their data.          | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                               |
| dc:instance:getConfiguration     | Grants permission to query DCS instance configuration parameters.        | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                               |
| dc:instance:modifyConfiguration  | Grants permission to modify DCS instance configuration parameters.       | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:modifyConfiguration |
| dc:instance:deleteDataBackupFile | Grants permission to delete DCS instance backup data.                    | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                               |
| dc:instance:restoreData          | Grants permission to restore DCS instance data.                          | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                               |

| Action                         | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|--------------------------------|--------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| dc:instance:getDataRestoreLog  | Grants permission to query DCS instance restoration records. | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| dc:instance:downloadBackupData | Grants permission to obtain backup file URLs.                | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| dc:instance:backupData         | Grants permission to back up DCS instance data.              | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| dc:instance:getDataBackupLog   | Grants permission to query DCS instance backup records.      | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| dc:migrationTask:create        | Grants permission to create data migration tasks.            | Write        | -                           | -                                     | -     |
| dc:migrationTask:list          | Grants permission to query data migration tasks.             | List         | -                           | -                                     | -     |
| dc:migrationTask:delete        | Grants permission to delete data migration tasks.            | Write        | migrationTask               | -                                     | -     |
| dc:migrationTask:get           | Grants permission to query data migration tasks.             | Read         | migrationTask *             | -                                     | -     |

| Action                                 | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                         | Alias                       |
|----------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------|
| dcsmigrationTask:modify                | Grants permission to configure and stop data migration tasks. | Write        | migrationTask *             | -                                     | dcsmigrationTask:exchangeIp |
| dcsinstance:listBigKey                 | Grants permission to query big keys.                          | List         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dcsinstance:analyze         |
| dcsinstance:getBigKey                  | Grants permission to query big key details.                   | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dcsinstance:analyze         |
| dcsinstance:deleteBigKeyScanTask       | Grants permission to delete big key scan tasks.               | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | dcsinstance:analyze         |
| dcsinstance:updateBigKeyAutoScanConfig | Grants permission to reschedule big key scan tasks.           | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dcsinstance:analyze         |
| dcsinstance:getBigKeyAutoScanConfig    | Grants permission to query scheduled big key scan tasks.      | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dcsinstance:analyze         |
| dcsinstance:analyzeHotKey              | Grants permission to perform hot key analysis.                | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dcsinstance:analyze         |
| dcsinstance:listHotKey                 | Grants permission to query hot keys.                          | List         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dcsinstance:analyze         |

| Action                                 | Description                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias               |
|----------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------|
| dc:instance:getHotKey                  | Grants permission to query hot key details.                               | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:analyze |
| dc:instance:deleteHotKeyScanTask       | Grants permission to delete hot key scan tasks.                           | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | dc:instance:analyze |
| dc:instance:updateHotKeyAutoScanConfig | Grants permission to reschedule hot key scan tasks.                       | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:analyze |
| dc:instance:getHotKeyAutoScanConfig    | Grants permission to query scheduled hot key scan tasks.                  | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:analyze |
| dc:instance:analyzeExpiredKey          | Grants permission to perform expired key analysis.                        | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:analyze |
| dc:instance:getAutoExpiredKeyScanTask  | Grants permission to query expired key scan tasks.                        | Read         | instance *                  | -                                     | dc:instance:analyze |
| dc:instance:updateExpiredKeyScanConfig | Grants permission to modify instance expired key scan task configuration. | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:analyze |



| Action                              | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                         | Alias               |
|-------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------|
| dc:instance:getExpiredKeyScanConfig | Grants permission to query instance expired key scan task configuration. | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:analyze |
| dc:slowlog:list                     | Grants permission to query slow query logs.                              | List         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                   |
| dc:aclaccount:create                | Grants permission to create ACL accounts.                                | Write        | instance *                  | -                                     | -                   |
| dc:aclaccount:list                  | Grants permission to query ACL accounts.                                 | List         | instance *                  | -                                     | -                   |
| dc:aclaccount:modify                | Grants permission to modify the passwords of ACL accounts.               | Write        | instance *                  | -                                     | -                   |
| dc:aclaccount:delete                | Grants permission to delete ACL accounts.                                | Write        | instance *                  | -                                     | -                   |
| dc:whitelist:modify                 | Grants permission to configure IP address whitelist groups.              | Write        | instance *                  | -                                     | -                   |
| dc:whitelist:list                   | Grants permission to query the IP address whitelist of instances.        | List         | instance *                  | -                                     | -                   |

| Action                           | Description                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                 |
|----------------------------------|-------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------|
| dc:instance:getBackgroundTask    | Grants permission to query background tasks.    | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                     |
| dc:instance:deleteBackgroundTask | Grants permission to delete background tasks.   | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -                     |
| dc:instance:createDiagnosisTask  | Grants permission to diagnose DCS instances.    | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:diagnosis |
| dc:instance:listDiagnosisTask    | Grants permission to query diagnosis tasks.     | List         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:diagnosis |
| dc:instance:getDiagnosisTask     | Grants permission to query diagnosis details.   | Read         | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:diagnosis |
| dc:instance:deleteDiagnosisTask  | Grants permission to delete diagnosis record.   | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | dc:instance:diagnosis |
| dc:template:list                 | Grants permission to query parameter templates. | List         | -                           | -                                     | -                     |
| dc:template:create               | Grants permission to customize templates.       | Write        | -                           | -                                     | -                     |

| Action              | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|---------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| dcg:template:get    | Grants permission to query parameter template.              | Read         | -                           | -                                                                                                                                     | -     |
| dcg:template:modify | Grants permission to modify customized parameter templates. | Write        | -                           | -                                                                                                                                     | -     |
| dcg:template:delete | Grants permission to delete customized parameter templates. | Write        | -                           | -                                                                                                                                     | -     |
| dcg:tag:list        | Grants permission to query all tags in your tenant account. | List         | -                           | -                                                                                                                                     | -     |
| dcg:tag:modify      | Grants permission to add or delete tags in batches.         | Write        | instance *                  | -                                                                                                                                     | -     |
|                     |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| dcg:tag:get         | Grants permission to query tags of instances.               | Read         | instance *                  | -                                                                                                                                     | -     |
|                     |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| dcg:redisLog:get    | Grants permission to obtain log download URLs.              | Read         | instance *                  | -                                                                                                                                     | -     |

| Action                  | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias                   |
|-------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------|
| dc:quota:get            | Grants permission to query tenant quotas.                                                 | Read         | -                           | -             | -                       |
| dc:instance:webcli      | Grants permission to connect DCS instances with WebCli.                                   | Write        | instance *                  | -             | -                       |
| dc:clientiptrans:modify | Grants permission to enables or disables transparent transmission of client IP addresses. | Write        | instance *                  | -             | dc:clientiptrans:modify |
| dc:clients:list         | Grants permission to query redis client list.                                             | Read         | instance *                  | -             | -                       |
| dc:clients:kill         | Grants permission to kill redis client.                                                   | Write        | instance *                  | -             | -                       |
| dc:ssl:get              | Grants permission to obtain SSL certificate information.                                  | Read         | instance *                  | -             | -                       |
| dc:ssl:modify           | Grants permission to modify SSL switch configuration.                                     | Write        | instance *                  | -             | -                       |
| dc:job:get              | Grants permission to obtain predecessor check results.                                    | Read         | -                           | -             | -                       |

| Action          | Description                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------|-------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dcg:task:list   | Grants permission to obtain the background task list. | List         | -                           | -             | -     |
| dcg:task:delete | Grants permission to delete background task records.  | Write        | -                           | -             | -     |

Each API of DCS usually supports one or more actions. [Table 3-219](#) lists the supported actions and dependencies.

**Table 3-219** Actions and dependencies supported by DCS APIs

| API                                          | Action              | Dependencies                                                                                                                                                                                                                               |
|----------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/instances              | dcg:instance:create | <ul style="list-style-type: none"> <li>vpc:ports:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>vpc:ports:delete</li> <li>vpc:subnets:get</li> <li>vpc:securityGroupRules:get</li> <li>vpc:securityGroups:get</li> </ul> |
| GET /v2/{project_id}/instances               | dcg:instance:list   | -                                                                                                                                                                                                                                          |
| DELETE /v2/{project_id}/instances            | dcg:instance:delete | <ul style="list-style-type: none"> <li>vpc:ports:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>vpc:ports:delete</li> <li>vpc:subnets:get</li> </ul>                                                                     |
| GET /v2/{project_id}/instances/{instance_id} | dcg:instance:get    | -                                                                                                                                                                                                                                          |

| API                                                            | Action                     | Dependencies                                                                                                                                                                                                                               |
|----------------------------------------------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v2/{project_id}/instances/{instance_id}                | dc:instance:delete         | <ul style="list-style-type: none"> <li>vpc:ports:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>vpc:ports:delete</li> <li>vpc:subnets:get</li> </ul>                                                                     |
| PUT /v2/{project_id}/instances/{instance_id}                   | dc:instance:modify         | <ul style="list-style-type: none"> <li>vpc:ports:get</li> <li>vpc:ports:update</li> </ul>                                                                                                                                                  |
| POST /v2/{project_id}/instances/{instance_id}/resize           | dc:instance:scale          | <ul style="list-style-type: none"> <li>vpc:ports:get</li> <li>vpc:ports:create</li> <li>vpc:ports:update</li> <li>vpc:ports:delete</li> <li>vpc:subnets:get</li> <li>vpc:securityGroupRules:get</li> <li>vpc:securityGroups:get</li> </ul> |
| POST /v2/{project_id}/instances/{instance_id}/resize/check-job | dc:instance:scale          | -                                                                                                                                                                                                                                          |
| POST /v2/{project_id}/instances/{instance_id}/swap             | dc:instance:swap           | -                                                                                                                                                                                                                                          |
| PUT /v2/{project_id}/instances/{instance_id}/password          | dc:instance:modifyAuthInfo | -                                                                                                                                                                                                                                          |
| POST /v2/{project_id}/instances/{instance_id}/password/reset   | dc:instance:modifyAuthInfo | -                                                                                                                                                                                                                                          |
| GET /v2/{project_id}/instances/status                          | dc:instance:list           | -                                                                                                                                                                                                                                          |
| PUT /v2/{project_id}/instances/status                          | dc:instance:modifyStatus   | -                                                                                                                                                                                                                                          |

| API                                                                                                   | Action                                | Dependencies |
|-------------------------------------------------------------------------------------------------------|---------------------------------------|--------------|
| GET /v2/{project_id}/instances/statistic                                                              | dcs:instance:list                     | -            |
| POST /v2/{project_id}/instances/{instance_id}/groups/{group_id}/replications/{node_id}/slave-priority | dcs:instance:modify                   | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/groups/{group_id}/replications/{node_id}/remove-ip    | dcs:instance:delete                   | -            |
| GET /v2/{project_id}/instance/{instance_id}/groups                                                    | dcs:instance:get                      | -            |
| GET /v2/{project_id}/instances/{instance_id}/configs                                                  | dcs:instance:getConfigurati<br>on     | -            |
| PUT /v2/{project_id}/instances/{instance_id}/configs                                                  | dcs:instance:modifyConfigur<br>ation  | -            |
| PUT /v2/{project_id}/instances/{instance_id}/async-configs                                            | dcs:instance:modifyConfigur<br>ation  | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/backups/{backup_id}                                   | dcs:instance:deleteDataBac<br>kupFile | -            |

| API                                                                     | Action                          | Dependencies |
|-------------------------------------------------------------------------|---------------------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/restores                  | dcs:instance:restoreData        | -            |
| GET /v2/{project_id}/instances/{instance_id}/restores                   | dcs:instance:getDataRestore Log | -            |
| POST /v2/{project_id}/instances/{instance_id}/backups/{backup_id}/links | dcs:instance:downloadBackupData | -            |
| POST /v2/{project_id}/instances/{instance_id}/backups                   | dcs:instance:backupData         | -            |
| GET /v2/{project_id}/instances/{instance_id}/backups                    | dcs:instance:getDataBackup Log  | -            |
| POST /v2/{project_id}/migration-task                                    | dcs:migrationTask:create        | -            |
| GET /v2/{project_id}/migration-tasks                                    | dcs:migrationTask:list          | -            |
| DELETE /v2/{project_id}/migration-tasks/delete                          | dcs:migrationTask:delete        | -            |
| GET /v2/{project_id}/migration-task/{task_id}                           | dcs:migrationTask:get           | -            |
| POST /v2/{project_id}/migration-task/{task_id}/stop                     | dcs:migrationTask:modify        | -            |



| API                                                          | Action                                  | Dependencies |
|--------------------------------------------------------------|-----------------------------------------|--------------|
| GET /v2/{project_id}/migration-task/{task_id}/stats          | dcs:migrationTask:get                   | -            |
| POST /v2/{project_id}/migration/instance                     | dcs:migrationTask:create                | -            |
| POST /v2/{project_id}/migration/{task_id}/task               | dcs:migrationTask:modify                | -            |
| POST /v2/{project_id}/migration-task/batch-stop              | dcs:migrationTask:modify                | -            |
| POST /v2/{project_id}/migration-task/{task_id}/sync-stop     | dcs:migrationTask:modify                | -            |
| GET /v2/{project_id}/dcs/tags                                | dcs:tag:list                            | -            |
| POST /v2/{project_id}/dcs/{instance_id}/tags/action          | dcs:tag:modify                          | -            |
| GET /v2/{project_id}/instances/{instance_id}/tags            | dcs:tag:get                             | -            |
| GET /v2/{project_id}/instances/{instance_id}/bigkey-tasks    | dcs:instance:listBigKey                 | -            |
| PUT /v2/{project_id}/instances/{instance_id}/bigkey/autoscan | dcs:instance:updateBigKeyAutoScanConfig | -            |

| API                                                                     | Action                                  | Dependencies |
|-------------------------------------------------------------------------|-----------------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/bigkey/autoscan            | dcs:instance:getBigKeyAutoScanConfig    | -            |
| POST /v2/{project_id}/instances/{instance_id}/hotkey-task               | dcs:instance:analyzeHotKey              | -            |
| GET /v2/{project_id}/instances/{instance_id}/hotkey-tasks               | dcs:instance:listHotKey                 | -            |
| GET /v2/{project_id}/instances/{instance_id}/hotkey-task/{hotkey_id}    | dcs:instance:getHotKey                  | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/hotkey-task/{hotkey_id} | dcs:instance:deleteHotKeyScanTask       | -            |
| PUT /v2/{project_id}/instances/{instance_id}/hotkey/autoscan            | dcs:instance:updateHotKeyAutoScanConfig | -            |
| GET /v2/{project_id}/instances/{instance_id}/hotkey/autoscan            | dcs:instance:getHotKeyAutoScanConfig    | -            |
| POST /v2/{project_id}/instances/{instance_id}/scan-expire-keys-task     | dcs:instance:analyzeExpiredKey          | -            |

| API                                                                           | Action                                  | Dependencies |
|-------------------------------------------------------------------------------|-----------------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/auto-expire/histories            | dcs:instance:getAutoExpiredKeyScanTask  | -            |
| POST /v2/{project_id}/instances/{instance_id}/auto-expire/scan                | dcs:instance:analyzeExpiredKey          | -            |
| GET /v2/{project_id}/instances/{instance_id}/scan-expire-keys/autoscan-config | dcs:instance:getExpiredKeyScanConfig    | -            |
| PUT /v2/{project_id}/instances/{instance_id}/scan-expire-keys/autoscan-config | dcs:instance:updateExpiredKeyScanConfig | -            |
| GET /v2/{project_id}/instances/{instance_id}/slowlog                          | dcs:slowlog:list                        | -            |
| GET /v2/{project_id}/instances/{instance_id}/redislog                         | dcs:redisLog:get                        | -            |
| POST /v2/{project_id}/instances/{instance_id}/redislog                        | dcs:redisLog:get                        | -            |
| POST /v2/{project_id}/instances/{instance_id}/redislog/{id}/links             | dcs:redisLog:get                        | -            |

| API                                                                                                        | Action                | Dependencies |
|------------------------------------------------------------------------------------------------------------|-----------------------|--------------|
| POST /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>accounts                                     | dcs:aclaccount:create | -            |
| GET /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>accounts                                      | dcs:aclaccount:list   | -            |
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>accounts/<br>{account_id}/<br>password/modify | dcs:aclaccount:modify | -            |
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>accounts/<br>{account_id}/<br>password/reset  | dcs:aclaccount:modify | -            |
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>accounts/<br>{account_id}                     | dcs:aclaccount:modify | -            |
| PUT /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>accounts/<br>{account_id}/role                | dcs:aclaccount:modify | -            |
| DELETE /v2/<br>{project_id}/<br>instances/<br>{instance_id}/<br>accounts/<br>{account_id}                  | dcs:aclaccount:delete | -            |

| API                                                             | Action                            | Dependencies |
|-----------------------------------------------------------------|-----------------------------------|--------------|
| PUT /v2/{project_id}/instance/{instance_id}/whitelist           | dcs:whitelist:modify              | -            |
| GET /v2/{project_id}/instance/{instance_id}/whitelist           | dcs:whitelist:list                | -            |
| GET /v2/{project_id}/instances/{instance_id}/tasks              | dcs:instance:getBackgroundTask    | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/tasks/{task_id} | dcs:instance:deleteBackgroundTask | -            |
| GET /v2/{project_id}/quota                                      | dcs:quota:get                     | -            |
| GET /v2/{project_id}/dms/monitored-objects/{instance_id}        | dcs:instance:get                  | -            |
| GET /v2/{project_id}/dms/monitored-objects                      | dcs:instance:list                 | -            |
| POST /v2/{project_id}/instances/{instance_id}/diagnosis         | dcs:instance:createDiagnosisTask  | -            |
| GET /v2/{project_id}/instances/{instance_id}/diagnosis          | dcs:instance:listDiagnosisTask    | -            |
| GET /v2/{project_id}/diagnosis/{report_id}                      | dcs:instance:getDiagnosisTask     | -            |

| API                                                           | Action                           | Dependencies |
|---------------------------------------------------------------|----------------------------------|--------------|
| DELETE /v2/{project_id}/instances/{instance_id}/diagnosis     | dcs:instance:deleteDiagnosisTask | -            |
| GET /v2/{project_id}/config-templates                         | dcs:template:list                | -            |
| POST /v2/{project_id}/config-templates                        | dcs:template:create              | -            |
| GET /v2/{project_id}/config-templates/{template_id}           | dcs:template:get                 | -            |
| DELETE /v2/{project_id}/config-templates/{template_id}        | dcs:template:delete              | -            |
| PUT /v2/{project_id}/config-templates/{template_id}           | dcs:template:modify              | -            |
| GET /v2/{project_id}/instances-logical-nodes                  | dcs:instance:list                | -            |
| GET /v2/{project_id}/instances/{instance_id}/config-histories | dcs:instance:get                 | -            |
| PUT /v2/{project_id}/instances/{instance_id}/bandwidth        | dcs:instance:modify              | -            |
| PUT /v2/{project_id}/instances/{instance_id}/async-swap       | dcs:instance:swap                | -            |

| API                                                                     | Action                            | Dependencies |
|-------------------------------------------------------------------------|-----------------------------------|--------------|
| GET /v2/{project_id}/instances/{instance_id}/operations                 | dcs:instance:get                  | -            |
| POST /v2/{project_id}/instances/{instance_id}/webcli/auth               | dcs:instance:webcli               | -            |
| POST /v2/{project_id}/instances/{instance_id}/webcli/command            | dcs:instance:webcli               | -            |
| POST /v2/{project_id}/instances/{instance_id}/webcli/logout             | dcs:instance:webcli               | -            |
| PUT /v2/{project_id}/{instance_id}/client-ip-transparent-transmission   | dcs:clientIpTrans:modify          | -            |
| GET /v2/{project_id}/instances/{instance_id}/bigkey-task/{bigkey_id}    | dcs:instance:getBigKey            | -            |
| DELETE /v2/{project_id}/instances/{instance_id}/bigkey-task/{bigkey_id} | dcs:instance:deleteBigKeyScanTask | -            |
| POST /v2/{project_id}/instances/{instance_id}/clients                   | dcs:clients:list                  | -            |
| GET /v2/{project_id}/instances/{instance_id}/clients                    | dcs:clients:list                  | -            |

| API                                                                                                    | Action             | Dependencies |
|--------------------------------------------------------------------------------------------------------|--------------------|--------------|
| POST /v2/{project_id}/instances/{instance_id}/clients/kill                                             | dcs:clients:kill   | -            |
| POST /v2/{project_id}/instances/{instance_id}/clients/kill-all                                         | dcs:clients:kill   | -            |
| GET /v2/{project_id}/instances/{instance_id}/config-histories/{history_id}                             | dcs:instance:get   | -            |
| GET /v2/{project_id}/instances/{instance_id}/deletable-replication                                     | dcs:instance:scale | -            |
| POST /v2/{project_id}/instances/export                                                                 | dcs:instance:list  | -            |
| GET /v2/{project_id}/instance/{instance_id}/groups/{group_id}/group-nodes-state                        | dcs:instance:get   | -            |
| POST /v2/{project_id}/instance/{instance_id}/groups/{group_id}/replications/{node_id}/async-switchover | dcs:instance:swap  | -            |
| GET /v2/{project_id}/instances/{instance_id}/ssl                                                       | dcs:ssl:get        | -            |



| API                                                                   | Action                          | Dependencies |
|-----------------------------------------------------------------------|---------------------------------|--------------|
| PUT /v2/{project_id}/instances/{instance_id}/ssl                      | dcs:ssl:modify                  | -            |
| POST /v2/{project_id}/instances/{instance_id}/ssl-certs/download      | dcs:ssl:modify                  | -            |
| GET /v2/{project_id}/instances/{instance_id}/tasks/{task_id}/progress | dcs:instance:getBackground Task | -            |
| GET /v2/{project_id}/instances/export-job                             | dcs:instance:exportListFile     | -            |
| GET /v2/{project_id}/jobs/{job_id}                                    | dcs:job:get                     | -            |
| PUT /v2/{project_id}/migration-task/{task_id}                         | dcs:migrationTask:modify        | -            |
| POST /v2/{project_id}/migration-task/{task_id}/exchange-ip            | dcs:migrationTask:modify        | -            |
| -                                                                     | dcs:instance:scale              | -            |
| GET /v2/{project_id}/tasks                                            | dcs:task:list                   | -            |
| DELETE /v2/{project_id}/tasks/{task_id}                               | dcs:task:delete                 | -            |
| GET /v2/{project_id}/migration-task/{task_id}/logs                    | dcs:migrationTask:get           | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-220](#), the resource URN must be

specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DCS.

**Table 3-220** Resource types supported by DCS

| Resource Type | URN                                             |
|---------------|-------------------------------------------------|
| instance      | dc<region>:<account-id>:instance:<instance-id>  |
| migrationTask | dc<region>:<account-id>:migrationTask:<task-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see **Global Condition Keys**.
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, dcs) apply only to operations of the xx service. For details, see **Table 3-221**.
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see **operators**.

### Service-specific condition keys supported by DCS

The following table lists the condition keys that you can define in identity policies for DCS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-221** Service-specific condition keys supported by DCS

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                     |
|--------------------------------|---------|-------------------------------|-----------------------------------------------------------------|
| dcs:backupEnabled              | boolean | Single-valued                 | Filters access for enabling automatic backup for DCS instances. |

## 3.11 Developer Services

### 3.11.1 ServiceStage

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your policy statements.

- If this column includes a resource type, you must specify the URN in the Resource element of your statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by ServiceStage, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by ServiceStage, see [Condition](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for ServiceStage.

**Table 3-222** Actions supported by ServiceStage

| Action                             | Description             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                   |
|------------------------------------|-------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| servicestage:app:getApplication    | Querying an application | read         | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | servicestage:app:get    |
| servicestage:app:createApplication | Creating an application | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | servicestage:app:create |

| Action                             | Description                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                 |
|------------------------------------|------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| servicetag:app:modifyApplication   | Updating an application            | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | servicetag:app:modify |
| servicetag:app:deleteApplication   | Deleting an application            | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | servicetag:app:delete |
| servicetag:app:listApplication     | Querying the application list      | list         | -                           | -                                                                                                                                                                                                                                               | servicetag:app:list   |
| servicetag:app:getConfiguration    | Querying application configuration | read         | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | servicetag:app:get    |
| servicetag:app:deleteConfiguration | Deleting application configuration | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | servicetag:app:modify |
| servicetag:app:modifyConfiguration | Updating application configuration | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | servicetag:app:modify |

| Action                         | Description                             | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias                 |
|--------------------------------|-----------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| servicetag:app:getComponent    | Querying an application component       | read         | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | servicetag:app:get    |
| servicetag:app:createComponent | Creating an application component       | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | servicetag:app:create |
| servicetag:app:modifyComponent | Updating an application component       | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | servicetag:app:modify |
| servicetag:app:deleteComponent | Deleting an application component       | write        | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | servicetag:app:delete |
| servicetag:app:listComponent   | Querying the application component list | list         | -                           | -                                                                                                                                                                                      | servicetag:app:list   |
| servicetag:environment:create  | Creating an environment                 | write        | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -                     |

| Action                           | Description                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                 |
|----------------------------------|-------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| servicetag:e:environment:get     | Querying an environment       | read         | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | -                     |
| servicetag:e:environment:list    | Querying the environment list | list         | -                           | -                                                                                                                                                                                                                                               | servicetag:e:app:list |
| servicetag:e:environment:modify  | Updating an environment       | write        | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -                     |
| servicetag:e:environment:delete  | Deleting an environment       | write        | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | -                     |
| servicetag:e:environment:refresh | Updating an environment       | write        | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                                                                              | -                     |

| Action                                         | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                         |
|------------------------------------------------|---------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| servicetag<br>e:environment:tag                | (TMS users)<br>Creating an environment tag  | tagging      | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | servicetag:environment:modify |
| servicetag<br>e:app:tag                        | (TMS users)<br>Creating an application tag  | tagging      | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | servicetag:app:modify         |
| servicetag<br>e:environment:listResourcesByTag | (TMS users)<br>Querying environments by tag | read         | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                           | servicetag:environment:list   |
| servicetag<br>e:app:listResourcesByTag         | (TMS users)<br>Querying applications by tag | read         | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                                           | servicetag:app:list           |
| servicetag<br>e:environment:unTagResource      | (TMS users)<br>Deleting an environment tag  | tagging      | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | servicetag:environment:modify |



| Action                               | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                   | Alias                         |
|--------------------------------------|--------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| servicetag:e:app:unTagResource       | (TMS users)<br>Deleting an application tag       | tagging      | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | servicetag:e:app:modify       |
| servicetag:e:environment:listTags    | (TMS users)<br>Querying the environment tag list | read         | -                           | -                                                                                                                                                                                                                                               | servicetag:e:environment:list |
| servicetag:e:app:listTags            | (TMS users)<br>Querying the application tag list | read         | -                           | -                                                                                                                                                                                                                                               | servicetag:e:app:list         |
| servicetag:e:environment:createAddon | Creating a plug-in                               | write        | -                           | -                                                                                                                                                                                                                                               | -                             |
| servicetag:e:environment:listAddon   | Querying a plug-in list                          | list         | -                           | -                                                                                                                                                                                                                                               | -                             |
| servicetag:e:environment:getAddon    | Querying the plug-in details                     | read         | -                           | -                                                                                                                                                                                                                                               | -                             |
| servicetag:e:environment:modifyAddon | Modifying a plug-in                              | write        | -                           | -                                                                                                                                                                                                                                               | -                             |
| servicetag:e:environment:deleteAddon | Deleting a plug-in                               | write        | -                           | -                                                                                                                                                                                                                                               | -                             |

| Action                        | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|-------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| servicetag:config:createGroup | Creating a configuration group                                              | write        | configGroup                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -     |
| servicetag:config:getGroup    | Obtaining group details based on the configured group ID                    | read         | configGroup                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| servicetag:config:listGroup   | Configuring group permissions                                               | list         | -                           | -                                                                                                                                                                                      | -     |
| servicetag:config:deleteGroup | Deleting a group based on the group ID                                      | write        | configGroup                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | -     |
| servicetag:config:get         | Obtaining configuration file information based on the configuration file ID | read         | config                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| servicetag:config:list        | Obtaining the configuration file information                                | list         | -                           | -                                                                                                                                                                                      | -     |

| Action                                | Description                                                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|---------------------------------------|------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| servicetag:<br>e:config:create        | Creating a configuration file                                                                  | write        | config                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -     |
| servicetag:<br>e:config:modify        | Modifying a configuration file based on the configuration file ID                              | write        | config                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| servicetag:<br>e:config:delete        | Deleting a configuration file based on the configuration file ID                               | write        | config                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| servicetag:<br>e:config:import        | Importing a configuration file                                                                 | write        | -                           | -                                                                                                                                                                                      | -     |
| servicetag:<br>e:config:listHistories | Obtaining configuration file history based on the configuration file ID                        | list         | config                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |
| servicetag:<br>e:config:getHistory    | Obtaining configuration file historical information based on the configuration file history ID | read         | config                      | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  | -     |

| Action                                 | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|----------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| servicetag e::config:deleteHistory     | Deleting configuration file history based on the configuration file history ID | write        | config                      | <a href="#">g:EnterpriseProjectId</a> | -     |
| servicetag e::getRuntimeStack          | Querying a technology stack based on the technology stack ID                   | read         | -                           | -                                     | -     |
| servicetag e::createRuntimeStack       | Creating a technology stack                                                    | write        | -                           | -                                     | -     |
| servicetag e::modifyRuntimeStack       | Modifying a technology stack based on the technology stack ID                  | write        | -                           | -                                     | -     |
| servicetag e::deleteRuntimeStack       | Deleting a technology stack based on the technology stack ID                   | write        | -                           | -                                     | -     |
| servicetag e::switchRuntimeStackStatus | Releasing a technology stack or canceling the release of a technology stack    | write        | -                           | -                                     | -     |
| servicetag e::vmappConfig:list         | Querying directory configurations                                              | list         | -                           | -                                     | -     |

| Action                          | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| servicetag e:vmappConfig:get    | Querying directory configurations based on the directory configuration ID  | read         | -                           | -             | -     |
| servicetag e:vmappConfig:create | Creating directory configurations                                          | write        | -                           | -             | -     |
| servicetag e:vmappConfig:modify | Modifying directory configurations based on the directory configuration ID | write        | -                           | -             | -     |
| servicetag e:vmappConfig:delete | Deleting directory configurations based on the directory configuration ID  | write        | -                           | -             | -     |
| servicetag e::createReleasePlan | Creating a release task                                                    | write        | -                           | -             | -     |
| servicetag e::getReleasePlan    | Obtaining information about a release task based on the release task ID    | read         | -                           | -             | -     |
| servicetag e::listReleasePlan   | Obtaining a release task list                                              | list         | -                           | -             | -     |

| Action                              | Description                                           | Access Level | Resource Type (*: required) | Condition Key         | Alias                       |
|-------------------------------------|-------------------------------------------------------|--------------|-----------------------------|-----------------------|-----------------------------|
| servicetag e::modifyReleasePlan     | Modifying a release task based on the release task ID | write        | -                           | -                     | -                           |
| servicetag e::deleteReleasePlan     | Deleting a release task based on the release task ID  | write        | -                           | -                     | -                           |
| servicetag e:pipeline:get           | Querying a pipeline                                   | read         | pipeline                    | g:EnterpriseProjectId | -                           |
| servicetag e:pipeline:create        | Creating a pipeline                                   | write        | pipeline                    | g:EnterpriseProjectId | -                           |
| servicetag e:pipeline:modify        | Updating a pipeline                                   | write        | pipeline                    | g:EnterpriseProjectId | -                           |
| servicetag e:pipeline:delete        | Deleting a pipeline                                   | write        | pipeline                    | g:EnterpriseProjectId | -                           |
| servicetag e:pipeline:list          | Querying the pipeline list                            | list         | -                           | -                     | -                           |
| servicetag e:assembling:runtimeList | Querying the technology stack list                    | read         | -                           | -                     | servicetag e:assembling:get |
| servicetag e:assembling:getInfo     | Querying a build task                                 | list         | -                           | -                     | -                           |
| servicetag e:assembling:create      | Creating a build task                                 | write        | assembling                  | -                     | -                           |
| servicetag e:assembling:modify      | Updating a build task                                 | write        | assembling                  | -                     | -                           |
| servicetag e:assembling:delete      | Deleting a build task                                 | write        | assembling                  | -                     | -                           |

| Action                                       | Description                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                 |
|----------------------------------------------|-----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| servicetag:e:assembling:list                 | Querying the build task list                  | list         | -                           | -                                                                                                                                                  | -                     |
| servicetag:e:repositoryAuth:list             | Obtaining the repository authorization list   | list         | -                           | -                                                                                                                                                  | -                     |
| servicetag:e:repositoryAuth:get              | Obtaining repository authorization            | read         | repositoryAuth              | -                                                                                                                                                  | -                     |
| servicetag:e:repositoryAuth:create           | Creating repository authorization             | write        | repositoryAuth              | -                                                                                                                                                  | -                     |
| servicetag:e:repositoryAuth:delete           | Deleting repository authorization             | write        | repositoryAuth              | -                                                                                                                                                  | -                     |
| servicetag:e:environment:listTagsForResource | (EPS users) Querying the environment tag list | read         | environment                 | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | servicetag:e:app:list |
| servicetag:e:app:listTagsForResource         | (EPS users) Querying the application tag list | read         | app                         | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | servicetag:e:app:list |

**Table 3-223** Actions supported by CSE

| Action                        | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias             |
|-------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| cse:config:upload             | Assigning permissions to upload microservice configurations                         | write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | cse:config:modify |
| cse:config:download           | Assigning permissions to download microservice configurations                       | write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | cse:config:modify |
| cse:engine:get                | Assigning permissions to view engines                                               | read         | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                 |
| cse:engine:list               | Assigning permissions to view the engine list                                       | list         | -                           | -                                                                                                                                              | -                 |
| cse:engine:backupRecover      | Assigning permissions to back up and restore engine data and change backup policies | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                 |
| cse:engine:associatePublicips | Assigning permissions to bind or unbind an engine to or from a public network       | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                 |



| Action               | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                          | Alias               |
|----------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| cse:engine:update    | Assigning permissions to modify the engine configuration and system management | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#"><i>g:ResourceTag/&lt;tag-key&gt;</i></a></li> <li><a href="#"><i>g:EnterpriseProjectId</i></a></li> </ul>                                           | -                   |
| cse:engine:create    | Assigning permissions to create an engine                                      | write        | -                           | <ul style="list-style-type: none"> <li><a href="#"><i>g:ResourceTag/&lt;tag-key&gt;</i></a></li> <li><a href="#"><i>g:EnterpriseProjectId</i></a></li> <li><a href="#"><i>g:TagKeys</i></a></li> </ul> | -                   |
| cse:engine:upgrade   | Assigning permissions to upgrade engine permissions                            | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#"><i>g:ResourceTag/&lt;tag-key&gt;</i></a></li> <li><a href="#"><i>g:EnterpriseProjectId</i></a></li> </ul>                                           | -                   |
| cse:engine:delete    | Assigning permissions to deleting an engine                                    | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#"><i>g:ResourceTag/&lt;tag-key&gt;</i></a></li> <li><a href="#"><i>g:EnterpriseProjectId</i></a></li> </ul>                                           | -                   |
| cse:namespace:get    | Assigning permissions to view namespaces                                       | read         | engine                      | <ul style="list-style-type: none"> <li><a href="#"><i>g:ResourceTag/&lt;tag-key&gt;</i></a></li> <li><a href="#"><i>g:EnterpriseProjectId</i></a></li> </ul>                                           | cse:namespace:read  |
| cse:namespace:update | Assigning permissions to modify namespace resources                            | write        | engine                      | <ul style="list-style-type: none"> <li><a href="#"><i>g:ResourceTag/&lt;tag-key&gt;</i></a></li> <li><a href="#"><i>g:EnterpriseProjectId</i></a></li> </ul>                                           | cse:namespace:write |

Each API of ServiceStage usually supports one or more actions. [Table 3-224](#) lists the actions and dependencies supported by ServiceStage APIs.

**Table 3-224** Actions and dependencies supported by ServiceStage APIs

| API                                                                     | Action                               | Dependencies |
|-------------------------------------------------------------------------|--------------------------------------|--------------|
| GET /v2/{project_id}/cas/metadata/runtimes                              | servicestage:app:listApplication     | -            |
| GET /v2/{project_id}/cas/metadata/flavors                               | servicestage:app:listApplication     | -            |
| POST /v2/{project_id}/cas/environments                                  | servicestage:environment:create      | -            |
| GET /v2/{project_id}/cas/environments                                   | servicestage:environment:list        | -            |
| PUT /v2/{project_id}/cas/environments/{environment_id}                  | servicestage:environment:modify      | -            |
| DELETE /v2/{project_id}/cas/environments/{environment_id}               | servicestage:environment:delete      | -            |
| GET /v2/{project_id}/cas/environments/{environment_id}                  | servicestage:environment:get         | -            |
| PATCH /v2/{project_id}/cas/environments/{environment_id}/resources      | servicestage:environment:modify      | -            |
| POST /v2/{project_id}/cas/applications                                  | servicestage:app:createApplication   | -            |
| GET /v2/{project_id}/cas/applications                                   | servicestage:app:listApplication     | -            |
| PUT /v2/{project_id}/cas/applications/{application_id}                  | servicestage:app:modifyApplication   | -            |
| DELETE /v2/{project_id}/cas/applications/{application_id}               | servicestage:app:deleteApplication   | -            |
| GET /v2/{project_id}/cas/applications/{application_id}                  | servicestage:app:getApplication      | -            |
| PUT /v2/{project_id}/cas/applications/{application_id}/configuration    | servicestage:app:modifyConfiguration | -            |
| DELETE /v2/{project_id}/cas/applications/{application_id}/configuration | servicestage:app:deleteConfiguration | -            |

| API                                                                                                              | Action                            | Dependencies                                                      |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------|
| GET /v2/{project_id}/cas/applications/{application_id}/configuration                                             | servicestage:app:getConfiguration | -                                                                 |
| POST /v2/{project_id}/cas/applications/{application_id}/components                                               | servicestage:app:createComponent  | servicestage:assembling:getInfo<br>servicestage:assembling:create |
| GET /v2/{project_id}/cas/applications/{application_id}/components                                                | servicestage:app:listComponent    | -                                                                 |
| PUT /v2/{project_id}/cas/applications/{application_id}/components/{component_id}                                 | servicestage:app:modifyComponent  | -                                                                 |
| DELETE /v2/{project_id}/cas/applications/{application_id}/components/{component_id}                              | servicestage:app:deleteComponent  | -                                                                 |
| GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}                                 | servicestage:app:getComponent     | -                                                                 |
| POST /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances                      | servicestage:app:createComponent  | servicestage:assembling:getInfo<br>servicestage:assembling:create |
| GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances                       | servicestage:app:listComponent    | -                                                                 |
| POST /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}/action | servicestage:app:modifyComponent  | -                                                                 |
| PUT /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}         | servicestage:app:modifyComponent  | -                                                                 |
| DELETE /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}      | servicestage:app:deleteComponent  | -                                                                 |

| API                                                                                                                | Action                             | Dependencies |
|--------------------------------------------------------------------------------------------------------------------|------------------------------------|--------------|
| GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}           | servicestage:app:getComponent      | -            |
| GET /v2/{project_id}/cas/applications/{application_id}/components/{component_id}/instances/{instance_id}/snapshots | servicestage:app:getComponent      | -            |
| GET /v2/{project_id}/cas/jobs/{job_id}                                                                             | servicestage:app:listApplication   | -            |
| POST /v3/{project_id}/cas/environments                                                                             | servicestage:environment:create    | -            |
| GET /v3/{project_id}/cas/environments                                                                              | servicestage:environment:list      | -            |
| PUT /v3/{project_id}/cas/environments/{environment_id}                                                             | servicestage:environment:modify    | -            |
| DELETE /v3/{project_id}/cas/environments/{environment_id}                                                          | servicestage:environment:delete    | -            |
| GET /v3/{project_id}/cas/environments/{environment_id}                                                             | servicestage:environment:get       | -            |
| PUT /v3/{project_id}/cas/environments/{environment_id}/resources                                                   | servicestage:environment:modify    | -            |
| GET /v3/{project_id}/cas/environments/{environment_id}/resources                                                   | servicestage:environment:list      | -            |
| POST /v3/{project_id}/cas/environments/{environment_id}/refresh                                                    | servicestage:environment:refresh   | -            |
| POST /v3/{project_id}/cas/applications                                                                             | servicestage:app:createApplication | -            |
| GET /v3/{project_id}/cas/applications                                                                              | servicestage:app:listApplication   | -            |
| PUT /v3/{project_id}/cas/applications/{application_id}                                                             | servicestage:app:modifyApplication | -            |
| GET /v3/{project_id}/cas/applications/{application_id}                                                             | servicestage:app:getApplication    | -            |
| DELETE /v3/{project_id}/cas/applications/{application_id}                                                          | servicestage:app:deleteApplication | -            |

| API                                                                                      | Action                               | Dependencies                                                      |
|------------------------------------------------------------------------------------------|--------------------------------------|-------------------------------------------------------------------|
| GET /v3/{project_id}/cas/applications/{application_id}/configuration                     | servicestage:app:getConfiguration    | -                                                                 |
| PUT /v3/{project_id}/cas/applications/{application_id}/configuration                     | servicestage:app:modifyConfiguration | -                                                                 |
| DELETE /v3/{project_id}/cas/applications/{application_id}/configuration                  | servicestage:app:deleteConfiguration | -                                                                 |
| POST /v3/{project_id}/cas/applications/{application_id}/components                       | servicestage:app:createComponent     | servicestage:assembling:getInfo<br>servicestage:assembling:create |
| GET /v3/{project_id}/cas/applications/{application_id}/components                        | servicestage:app:listComponent       | -                                                                 |
| GET /v3/{project_id}/cas/components                                                      | servicestage:app:listComponent       | -                                                                 |
| PUT /v3/{project_id}/cas/applications/{application_id}/components/{component_id}         | servicestage:app:modifyComponent     | -                                                                 |
| DELETE /v3/{project_id}/cas/applications/{application_id}/components/{component_id}      | servicestage:app:deleteComponent     | -                                                                 |
| GET /v3/{project_id}/cas/applications/{application_id}/components/{component_id}         | servicestage:app:getComponent        | -                                                                 |
| POST /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/action | servicestage:app:modifyComponent     | -                                                                 |
| GET /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/records | servicestage:app:listComponent       | -                                                                 |
| PUT /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/refresh | servicestage:app:modifyComponent     | -                                                                 |
| GET /v3/{project_id}/cas/components/filterOptions                                        | servicestage:app:listComponent       | -                                                                 |

| API                                                                                          | Action                            | Dependencies                                                      |
|----------------------------------------------------------------------------------------------|-----------------------------------|-------------------------------------------------------------------|
| POST /v3/{project_id}/cas/components                                                         | servicestage:app:createComponent  | servicestage:assembling:getInfo<br>servicestage:assembling:create |
| POST /v3/{project_id}/cas/components/parse-template-package                                  | servicestage:app:getComponent     | -                                                                 |
| PUT /v3/{project_id}/cas/applications/{application_id}/components/{component_id}/redployment | servicestage:app:modifyComponent  | -                                                                 |
| GET /v3/{project_id}/cas/jobs/{job_id}                                                       | servicestage:app:listApplication  | -                                                                 |
| POST /v3/{project_id}/cas/config-groups                                                      | servicestage:config:createGroup   | -                                                                 |
| GET /v3/{project_id}/cas/config-groups                                                       | servicestage:config:listGroup     | -                                                                 |
| POST /v3/{project_id}/cas/configs                                                            | servicestage:config:create        | -                                                                 |
| POST /v3/{project_id}/cas/configs/import                                                     | servicestage:config:import        | -                                                                 |
| GET /v3/{project_id}/cas/configs                                                             | servicestage:config:list          | -                                                                 |
| GET /v3/{project_id}/cas/configs/{config_id}                                                 | servicestage:config:get           | -                                                                 |
| DELETE /v3/{project_id}/cas/configs/{config_id}                                              | servicestage:config:delete        | -                                                                 |
| PUT /v3/{project_id}/cas/configs/{config_id}                                                 | servicestage:config:modify        | -                                                                 |
| GET /v3/{project_id}/cas/configs/{config_id}/histories                                       | servicestage:config:listHistories | -                                                                 |
| GET /v3/{project_id}/cas/configs/{config_id}/histories/{config_history_id}                   | servicestage:config:getHistory    | -                                                                 |
| DELETE /v3/{project_id}/cas/configs/{config_id}/histories/{config_history_id}                | servicestage:config:deleteHistory | -                                                                 |
| GET /v3/{project_id}/cas/config-groups/{config_group_id}                                     | servicestage:config:getGroup      | -                                                                 |

| API                                                                                          | Action                                   | Dependencies |
|----------------------------------------------------------------------------------------------|------------------------------------------|--------------|
| DELETE /v3/{project_id}/cas/<br>config-groups/<br>{config_group_id}                          | servicestage:config:del<br>eteGroup      | -            |
| POST /v3/{project_id}/cas/<br>environments/<br>{environment_id}/addons                       | servicestage:environm<br>ent:createAddon | -            |
| GET /v3/{project_id}/cas/<br>environments/<br>{environment_id}/addons                        | servicestage:environm<br>ent:listAddon   | -            |
| GET /v3/{project_id}/cas/<br>environments/<br>{environment_id}/addons-<br>metadata           | servicestage:environm<br>ent:listAddon   | -            |
| GET /v3/{project_id}/cas/<br>environments/<br>{environment_id}/addons/<br>{addon_id}         | servicestage:environm<br>ent:getAddon    | -            |
| POST /v3/{project_id}/cas/<br>environments/<br>{environment_id}/addons/<br>{addon_id}/action | servicestage:environm<br>ent:modifyAddon | -            |
| DELETE /v3/{project_id}/cas/<br>environments/<br>{environment_id}/addons/<br>{addon_id}      | servicestage:environm<br>ent:deleteAddon | -            |
| POST /v3/{project_id}/cas/<br>release-plans                                                  | servicestage::createRel<br>easePlan      | -            |
| PUT /v3/{project_id}/cas/<br>release-plans/{release_plan_id}                                 | servicestage::modifyRe<br>leasePlan      | -            |
| DELETE /v3/{project_id}/cas/<br>release-plans/{release_plan_id}                              | servicestage::deleteRel<br>easePlan      | -            |
| GET /v3/{project_id}/cas/<br>release-plans                                                   | servicestage::listReleas<br>ePlan        | -            |
| GET /v3/{project_id}/cas/<br>release-plans/{release_plan_id}                                 | servicestage::getRelea<br>sePlan         | -            |
| GET /v3/{project_id}/cas/<br>release-plans/{release_plan_id}/<br>deploy-info                 | servicestage::getRelea<br>sePlan         | -            |
| POST /v3/{project_id}/cas/<br>release-plans/{release_plan_id}/<br>execute                    | servicestage::createRel<br>easePlan      | -            |

| API                                                                        | Action                               | Dependencies |
|----------------------------------------------------------------------------|--------------------------------------|--------------|
| POST /v3/{project_id}/cas/<br>release-plans/{release_plan_id}/<br>rollback | servicestage::createRel<br>easePlan  | -            |
| POST /v3/{project_id}/cas/<br>release-plans/{release_plan_id}/<br>abort    | servicestage::createRel<br>easePlan  | -            |
| POST /v3/{project_id}/pipeline/<br>pipelines                               | servicestage:pipeline:c<br>reate     | -            |
| GET /v3/{project_id}/pipeline/<br>pipelines                                | servicestage:pipeline:li<br>st       | -            |
| PUT /v3/{project_id}/pipeline/<br>pipelines/{pipeline_id}                  | servicestage:pipeline:<br>modify     | -            |
| POST /v3/{project_id}/pipeline/<br>pipelines/{pipeline_id}/action          | servicestage:pipeline:<br>modify     | -            |
| GET /v3/{project_id}/pipeline/<br>pipelines/{pipeline_id}                  | servicestage:pipeline:g<br>et        | -            |
| GET /v3/{project_id}/pipeline/<br>pipelines/{id}/records                   | servicestage:pipeline:g<br>et        | -            |
| POST /v3/{project_id}/pipeline/<br>pipelines/{pipeline_id}/hooks           | servicestage:pipeline:c<br>reate     | -            |
| PUT /v3/{project_id}/pipeline/<br>pipelines/{pipeline_id}/hooks            | servicestage:pipeline:<br>modify     | -            |
| GET /v3/{project_id}/pipeline/<br>pipelines/{pipeline_id}/hooks            | servicestage:pipeline:li<br>st       | -            |
| POST /v3/{project_id}/pipeline/<br>pipelines/parse-template-<br>package    | servicestage:pipeline:g<br>et        | -            |
| POST /v3/{project_id}/cas/<br>runtimestacks                                | servicestage::createRu<br>ntimeStack | -            |
| GET /v3/{project_id}/cas/<br>runtimestacks                                 | servicestage:app:listAp<br>plication | -            |
| GET /v3/{project_id}/cas/<br>runtimestacks/<br>{runtimestack_id}           | servicestage::getRunti<br>meStack    | -            |
| PUT /v3/{project_id}/cas/<br>runtimestacks/<br>{runtimestack_id}           | servicestage::modifyR<br>untimeStack | -            |



| API                                                                         | Action                                               | Dependencies |
|-----------------------------------------------------------------------------|------------------------------------------------------|--------------|
| DELETE /v3/{project_id}/cas/<br>runtimestacks/<br>{runtimestack_id}         | servicestage::deleteRu<br>ntimeStack                 | -            |
| POST /v3/{project_id}/cas/<br>runtimestacks/action                          | servicestage::switchRu<br>ntimeStackStatus           | -            |
| GET /v3/{project_id}/cas/<br>innerimages                                    | servicestage:app:listAp<br>plication                 | -            |
| POST /v3/{project_id}/cas/<br>vmapp-configs                                 | servicestage:vmappCo<br>nfig:create                  | -            |
| GET /v3/{project_id}/cas/<br>vmapp-configs                                  | servicestage:vmappCo<br>nfig:list                    | -            |
| GET /v3/{project_id}/cas/<br>vmapp-configs/<br>{vmapp_config_id}            | servicestage:vmappCo<br>nfig:get                     | -            |
| PUT /v3/{project_id}/cas/<br>vmapp-configs/<br>{vmapp_config_id}            | servicestage:vmappCo<br>nfig:modify                  | -            |
| DELETE /v3/{project_id}/cas/<br>vmapp-configs/<br>{vmapp_config_id}         | servicestage:vmappCo<br>nfig:delete                  | -            |
| GET /v1/{project_id}/git/auths                                              | servicestage:repository<br>Auth:list                 | -            |
| GET /v1/{project_id}/git/auths/<br>{repo_type}/redirect                     | servicestage:repository<br>Auth:get                  | -            |
| POST /v1/{project_id}/git/<br>auths/{repo_type}/oauth                       | servicestage:repository<br>Auth:create               | -            |
| POST /v1/{project_id}/git/<br>auths/{repo_type}/personal                    | servicestage:repository<br>Auth:create               | -            |
| POST /v1/{project_id}/git/<br>auths/{repo_type}/password                    | servicestage:repository<br>Auth:create               | -            |
| DELETE /v1/{project_id}/git/<br>auths/{name}                                | servicestage:repository<br>Auth:delete               | -            |
| GET /v1/{project_id}/git/auths/<br>{repo_type}/password/valid               | servicestage:repository<br>Auth:get                  | -            |
| GET /v2/{project_id}/<br>servicestage-environment/<br>{environment_id}/tags | servicestage:environm<br>ent:listTagsForResourc<br>e | -            |

| API                                                              | Action                               | Dependencies |
|------------------------------------------------------------------|--------------------------------------|--------------|
| GET /v2/{project_id}/servicestage-application/{app_id}/tags      | servicestage:app:listTagsForResource | -            |
| POST /v1/{project_id}/kie/file                                   | cse:config:upload                    | -            |
| POST /v1/{project_id}/kie/download                               | cse:config:download                  | -            |
| GET /v2/{project_id}/enginemgr/engines                           | cse:engine:list                      | -            |
| POST /v2/{project_id}/enginemgr/engines                          | cse:engine:create                    | -            |
| GET /v2/{project_id}/enginemgr/engines/{engine_id}               | cse:engine:get                       | -            |
| DELETE /v2/{project_id}/enginemgr/engines/{engine_id}            | cse:engine:delete                    | -            |
| GET /v2/{project_id}/enginemgr/engines/{engine_id}/jobs/{job_id} | cse:engine:get                       | -            |
| POST /v1/{project_id}/kie/kv                                     | cse:namespace:update                 | -            |
| PUT /v1/{project_id}/kie/kv/{kv_id}                              | cse:namespace:update                 | -            |
| GET /v1/{project_id}/kie/kv                                      | cse:namespace:get                    | -            |
| DELETE /v1/{project_id}/kie/kv/{kv_id}                           | cse:namespace:update                 | -            |
| DELETE /v1/{project_id}/kie/kv                                   | cse:namespace:update                 | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-225](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for ServiceStage.

**Table 3-225** Resource types supported by ServiceStage

| Resource Type  | URN                                                                     |
|----------------|-------------------------------------------------------------------------|
| app            | servicestage:<region>:<account-id>:app:<app-id>                         |
| environment    | servicestage:<region>:<account-id>:environment:<environment-id>         |
| pipeline       | servicestage:<region>:<account-id>:pipeline:<pipeline-id>               |
| assembling     | servicestage:<region>:<account-id>:assembling:<assembling-id>           |
| repositoryAuth | servicestage:<region>:<account-id>:repositoryAuth:<repositoryAuth-id>   |
| configGroup    | servicestage:<region>:<account-id>:configGroup:<config-group-id>        |
| config         | servicestage:<region>:<account-id>:config:<config-group-id>/<config-id> |

## Condition

ServiceStage does not support service-specific condition keys in policies.

It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.11.2 CodeArts

The [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU.

This section describes the elements used by Organizations SCPs. The elements include actions, resources, and conditions.

For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an SCP.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an SCP.

- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions, and you must specify all resources ("\*") in your SCP statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by the CodeArts console, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an SCP statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by the CodeArts console, see [Conditions](#).

The following table lists the actions that you can define in SCP statements for the CodeArts console.

**Table 3-226** Actions supported by the CodeArts console

| Action                        | Description                                                             | Access Level | Resource Type (*: required) | Condition Key |
|-------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:projectman:viewUsage | Grants permission to check CodeArts Req resource usage on the console.  | read         | -                           | -             |
| codearts:codehub:viewUsage    | Grants permission to check CodeArts Repo resource usage on the console. | read         | -                           | -             |

| Action                          | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key |
|---------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:cloudbuild:viewUsage   | Grants permission to check CodeArts Build resource usage on the console.                      | read         | -                           | -             |
| codearts:codecheck:viewUsage    | Grants permission to check CodeArts Check resource usage on the console.                      | read         | -                           | -             |
| codearts:clouddtest:viewUsage   | Grants permission to check CodeArts TestPlan (Test Management) resource usage on the console. | read         | -                           | -             |
| codearts:apitest:viewUsage      | Grants permission to check CodeArts TestPlan (APITest) resource usage on the console.         | read         | -                           | -             |
| codearts:cloudrelease:viewUsage | Grants permission to check CodeArts Artifact resource usage on the console.                   | read         | -                           | -             |

| Action                                      | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key |
|---------------------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:cloudide:viewUsage                 | Grants permission to check CodeArts IDE resource usage on the console.              | read         | -                           | -             |
| codearts:classroom:viewUsage                | Grants permission to check Classroom resource usage on the console.                 | read         | -                           | -             |
| codearts:monthlyPackage:changeSpecification | Grants permission to change package specifications on the console.                  | write        | -                           | -             |
| codearts:monthlyPackage:subscribe           | Grants permission to purchase packages on the console.                              | write        | -                           | -             |
| codearts:projectman:subscribeService        | Grants permission to subscribe to CodeArts Req in pay-per-use mode on the console.  | write        | -                           | -             |
| codearts:codehub:subscribeService           | Grants permission to subscribe to CodeArts Repo in pay-per-use mode on the console. | write        | -                           | -             |

| Action                                 | Description                                                                                               | Access Level | Resource Type (*: required) | Condition Key |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:cloudbuild:subscribeService   | Grants permission to subscribe to CodeArts Build in pay-per-use mode on the console.                      | write        | -                           | -             |
| codearts:codecheck:subscribeService    | Grants permission to subscribe to CodeArts Check in pay-per-use mode on the console.                      | write        | -                           | -             |
| codearts:clouddtest:subscribeService   | Grants permission to subscribe to CodeArts TestPlan (Test Management) in pay-per-use mode on the console. | write        | -                           | -             |
| codearts:apitest:subscribeService      | Grants permission to subscribe to CodeArts TestPlan (APITest) in pay-per-use mode on the console.         | write        | -                           | -             |
| codearts:cloudrelease:subscribeService | Grants permission to subscribe to CodeArts Artifact in pay-per-use mode on the console.                   | write        | -                           | -             |

| Action                                 | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key |
|----------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:package:subscribeService      | Grants permission to subscribe to a pay-per-use package on the console.                 | write        | -                           | -             |
| codearts:cloudide:subscribeService     | Grants permission to subscribe to CodeArts IDE in pay-per-use mode on the console.      | write        | -                           | -             |
| codearts:classroom:subscribeService    | Grants permission to subscribe to Classroom in pay-per-use mode on the console.         | write        | -                           | -             |
| codearts:projectman:unsubscribeService | Grants permission to unsubscribe from CodeArts Req in pay-per-use mode on the console.  | write        | -                           | -             |
| codearts:codehub:unsubscribeService    | Grants permission to unsubscribe from CodeArts Repo in pay-per-use mode on the console. | write        | -                           | -             |



| Action                                 | Description                                                                                                   | Access Level | Resource Type (*: required) | Condition Key |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:cloudbuild:unsubscribeService | Grants permission to unsubscribe from CodeArts Build in pay-per-use mode on the console.                      | write        | -                           | -             |
| codearts:codecheck:unsubscribeService  | Grants permission to unsubscribe from CodeArts Check in pay-per-use mode on the console.                      | write        | -                           | -             |
| codearts:clouddtest:unsubscribeService | Grants permission to unsubscribe from CodeArts TestPlan (Test Management) in pay-per-use mode on the console. | write        | -                           | -             |
| codearts:apitest:unsubscribeService    | Grants permission to unsubscribe from CodeArts TestPlan (APITest) in pay-per-use mode on the console.         | write        | -                           | -             |

| Action                                       | Description                                                                                 | Access Level | Resource Type (*: required) | Condition Key |
|----------------------------------------------|---------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:cloudrelease:unsubscribeService     | Grants permission to unsubscribe from CodeArts Artifact in pay-per-use mode on the console. | write        | -                           | -             |
| codearts:package:unsubscribeService          | Grants permission to unsubscribe from a pay-per-use package on the console.                 | write        | -                           | -             |
| codearts:cloudide:unsubscribeService         | Grants permission to unsubscribe from CodeArts IDE in pay-per-use mode on the console.      | write        | -                           | -             |
| codearts:classroom:unsubscribeService        | Grants permission to unsubscribe from Classroom in pay-per-use mode on the console.         | write        | -                           | -             |
| codearts:authorization:list                  | Grants permission to view the authorization list on the console.                            | list         | -                           | -             |
| codearts:payPerUsePackage:listResourceDetail | Grants permission to view details of a pay-per-use package on the console.                  | list         | -                           | -             |

| Action                                     | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key |
|--------------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:monthlyPackage:listResourceDetail | Grants permission to view package resources on the console.                             | list         | -                           | -             |
| codearts:projectman:listResourceDetail     | Grants permission to view CodeArts Req resources on the console.                        | list         | -                           | -             |
| codearts:codehub:listResourceDetail        | Grants permission to view CodeArts Repo resources on the console.                       | list         | -                           | -             |
| codearts:cloudbuild:listResourceDetail     | Grants permission to view CodeArts Build resources on the console.                      | list         | -                           | -             |
| codearts:codecheck:listResourceDetail      | Grants permission to view CodeArts Check resources on the console.                      | list         | -                           | -             |
| codearts:clouddtest:listResourceDetail     | Grants permission to view CodeArts TestPlan (Test Management) resources on the console. | list         | -                           | -             |
| codearts:cloudrelease:listResourceDetail   | Grants permission to view CodeArts Artifact resources on the console.                   | list         | -                           | -             |

| Action                                                  | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:cloudide:listResourceDetail                    | Grants permission to view CodeArts IDE resources on the console.                             | list         | -                           | -             |
| codearts:classroom:listResourceDetail                   | Grants permission to view Classroom resources on the console.                                | list         | -                           | -             |
| codearts:agileDevopsTrainingServices:listResourceDetail | Grants permission to view resources of the Agile and DevOps Training Service on the console. | list         | -                           | -             |
| codearts:projectman:listSubscriptionHistory             | Grants permission to view CodeArts Req subscription history on the console.                  | list         | -                           | -             |
| codearts:codehub:listSubscriptionHistory                | Grants permission to view CodeArts Repo subscription history on the console.                 | list         | -                           | -             |
| codearts:cloudbuild:listSubscriptionHistory             | Grants permission to view CodeArts Build subscription history on the console.                | list         | -                           | -             |

| Action                                        | Description                                                                                        | Access Level | Resource Type (*: required) | Condition Key |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:codecheck:listSubscriptionHistory    | Grants permission to view CodeArts Check subscription history on the console.                      | list         | -                           | -             |
| codearts:cloudtest:listSubscriptionHistory    | Grants permission to view CodeArts TestPlan (Test Management) subscription history on the console. | list         | -                           | -             |
| codearts:apitest:listSubscriptionHistory      | Grants permission to view CodeArts TestPlan (APITest) subscription history on the console.         | list         | -                           | -             |
| codearts:cloudrelease:listSubscriptionHistory | Grants permission to view CodeArts Artifact subscription history on the console.                   | list         | -                           | -             |
| codearts:package:listSubscriptionHistory      | Grants permission to view pay-per-use package subscription history on the console.                 | list         | -                           | -             |
| codearts:cloudide:listSubscriptionHistory     | Grants permission to view CodeArts IDE subscription history on the console.                        | list         | -                           | -             |

| Action                                     | Description                                                                                    | Access Level | Resource Type (*: required) | Condition Key |
|--------------------------------------------|------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|
| codearts:classroom:listSubscriptionHistory | Grants permission to view Classroom subscription history on the console.                       | list         | -                           | -             |
| codearts:authorization:create              | Grants permission to authorize enterprise accounts on the console.                             | permissions  | -                           | -             |
| codearts:authorization:cancel              | Grants permission to cancel the authorization granted to enterprise accounts on the console.   | permissions  | -                           | -             |
| codearts:authorization:update              | Grants permission to accept or reject authorization from an enterprise account on the console. | permissions  | -                           | -             |

## Resources

The CodeArts console does not support resource-level authorization. To allow access to the CodeArts console, use a wildcard (\*) in the Resource element of the SCP, indicating that the SCP will be applied to all resources.

## Conditions

The CodeArts console does not support service-specific condition keys in SCPs.

It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.11.3 CodeArts Pipeline

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by CodeartsPipeline, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.

- If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by CodeartsPipeline, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for CodeartsPipeline.

**Table 3-227** Actions supported by CodeartsPipeline

| Action                                    | Description                                           | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                    |
|-------------------------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------------|
| codeartspipeline:pipeline-template:create | Grants permission to create a pipeline template.      | Write        | -                           | -             | -                                                                                        |
| codeartspipeline:pipeline-template:update | Grants permission to update a pipeline template.      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:pipeline-template:update</li> </ul> |
| codeartspipeline:pipeline-template:delete | Grants permission to delete a pipeline template.      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:pipeline-template:update</li> </ul> |
| codeartspipeline:pipeline-template:get    | Grants permission to view a pipeline template.        | Read         | -                           | -             | -                                                                                        |
| codeartspipeline:pipeline-template:list   | Grants permission to view the pipeline template list. | List         | -                           | -             | -                                                                                        |
| codeartspipeline:rule:create              | Grants permission to create a rule.                   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:rule:update</li> </ul>              |



| Action                            | Description                                      | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                               |
|-----------------------------------|--------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------------------------------------------------------|
| codeartspipeline:rule:update      | Grants permission to update a rule.              | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:rule:update</li> </ul>         |
| codeartspipeline:rule:delete      | Grants permission to delete a rule.              | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:rule:update</li> </ul>         |
| codeartspipeline:rule:get         | Grants permission to view a rule.                | Read         | -                           | -             | -                                                                                   |
| codeartspipeline:rule:list        | Grants permission to view the rule list.         | List         | -                           | -             | -                                                                                   |
| codeartspipeline:strategy:create  | Grants permission to create a strategy.          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:ruletemplate:update</li> </ul> |
| codeartspipeline:strategy:update  | Grants permission to update a strategy.          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:ruletemplate:update</li> </ul> |
| codeartspipeline:strategy:delete  | Grants permission to delete a strategy.          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:ruletemplate:update</li> </ul> |
| codeartspipeline:strategy:get     | Grants permission to view a strategy.            | Read         | -                           | -             | -                                                                                   |
| codeartspipeline:strategy:list    | Grants permission to view the strategy list.     | List         | -                           | -             | -                                                                                   |
| codeartspipeline:extension:create | Grants permission to create an extension plugin. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>cloudpipeline:extensions:update</li> </ul>   |

| Action                            | Description                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                           |
|-----------------------------------|----------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------|
| codeartspipeline:extension:update | Grants permission to update an extension plugin.   | Write        | -                           | -             | <ul style="list-style-type: none"><li>cloudpipeline:extensions:update</li></ul> |
| codeartspipeline:extension:delete | Grants permission to delete an extension plugin.   | Write        | -                           | -             | <ul style="list-style-type: none"><li>cloudpipeline:extensions:update</li></ul> |
| codeartspipeline:extension:get    | Grants permission to view an extension plugin.     | Read         | -                           | -             | -                                                                               |
| codeartspipeline:extension:list   | Grants permission to list all pipeline extensions. | List         | -                           | -             | -                                                                               |

## Resources

CodeartsPipeline does not support resource-level authorization. To allow access to CodeartsPipeline, use a wildcard (\*) in the Resource element of the identity policy, indicating that the identity policy will be applied to all resources.

## Conditions

CodeartsPipeline does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.11.4 Cloud Application Engine

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational

unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by cae, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by cae, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for cae.

**Table 3-228** Actions supported by CAE

| Action                            | Description                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|-----------------------------------|----------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| cae:environment:listEnvironments  | Grant permission to query all environments.  | List         | environment *               | -                                     | cae:environment:list   |
| cae:environment:createEnvironment | Grant permission to create an environment.   | Write        | environment *               | -                                     | cae:environment:create |
|                                   |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:deleteEnvironment | Grant permission to delete an environment.   | Write        | environment *               | -                                     | cae:environment:delete |
|                                   |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:getEnvironment    | Grant permission to query an environment.    | Read         | environment *               | -                                     | cae:environment:get    |
|                                   |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:listCloudVolumes  | Grant permission to query all cloud storage. | List         | environment *               | -                                     | cae:environment:list   |
|                                   |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:createCloudVolume | Grant permission to authorize cloud storage. | Write        | environment *               | -                                     | cae:environment:create |
|                                   |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:deleteCloudVolume | Grant permission to unbind cloud storage.    | Write        | environment *               | -                                     | cae:environment:delete |
|                                   |                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |

| Action                            | Description                                 | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|-----------------------------------|---------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| cae:environment:listDomains       | Grant permission to query all domain names. | List         | environment *               | -                                     | cae:environment:get    |
|                                   |                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:createDomain      | Grant permission to create a domain name.   | Write        | environment *               | -                                     | cae:environment:create |
|                                   |                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:deleteDomain      | Grant permission to delete a domain name.   | Write        | environment *               | -                                     | cae:environment:delete |
|                                   |                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:listCertificates  | Grant permission to query all certificates. | List         | environment *               | -                                     | cae:environment:get    |
|                                   |                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:createCertificate | Grant permission to create a certificate.   | Write        | environment *               | -                                     | cae:environment:create |
|                                   |                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:deleteCertificate | Grant permission to delete a certificate.   | Write        | environment *               | -                                     | cae:environment:delete |
|                                   |                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:updateCertificate | Grant permission to update a certificate.   | Write        | environment *               | -                                     | cae:environment:update |
|                                   |                                             |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |

| Action                          | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|---------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| cae:environment:listTimerRules  | Grant permission to query all start/stop rules.                                              | List         | environment *               | -                                     | cae:environment:get    |
|                                 |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:createTimerRule | Grant permission to create a start/stop rule.                                                | Write        | environment *               | -                                     | cae:environment:create |
|                                 |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:deleteTimerRule | Grant permission to delete a start/stop rule.                                                | Write        | environment *               | -                                     | cae:environment:delete |
|                                 |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:updateTimerRule | Grant permission to update a start/stop rule.                                                | Write        | environment *               | -                                     | cae:environment:update |
|                                 |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:getTimerRule    | Grant permission to query a start/stop rule.                                                 | Read         | environment *               | -                                     | cae:environment:get    |
|                                 |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:listEips        | Grant permission to view all EIPs (inter-access between the environment and public network). | List         | environment *               | -                                     | cae:environment:get    |
|                                 |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |

| Action                           | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|----------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| cae:environment:updateEip        | Grant permission to update an EIP (inter-access between the environment and public network). | Write        | environment *               | -                                     | cae:environment:update |
|                                  |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:listVpcEgresses  | Grant permission to view all VPC egresses.                                                   | List         | environment *               | -                                     | cae:environment:get    |
|                                  |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:createVpcEgress  | Grant permission to create a VPC egress.                                                     | Write        | environment *               | -                                     | cae:environment:create |
|                                  |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:deleteVpcEgress  | Grant permission to delete a VPC egress.                                                     | Write        | environment *               | -                                     | cae:environment:delete |
|                                  |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:listVpcIngresses | Grant permission to view all VPC ingresses.                                                  | List         | environment *               | -                                     | cae:environment:get    |
|                                  |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:createVpcIngress | Grant permission to create a VPC ingress.                                                    | Write        | environment *               | -                                     | cae:environment:create |
|                                  |                                                                                              |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:deleteVpcIngress | Grant permission to delete a VPC ingress.                                                    | Write        | environment *               | -                                     | cae:environment:delete |

| Action                              | Description                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|-------------------------------------|-------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
|                                     |                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:createMonitorSystem | Grant permission to create a monitoring system. | Write        | environment *               | -                                     | cae:environment:create |
|                                     |                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:updateMonitorSystem | Grant permission to update a monitoring system. | Write        | environment *               | -                                     | cae:environment:update |
|                                     |                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:environment:getMonitorSystem    | Grant permission to query a monitoring system.  | Read         | environment *               | -                                     | cae:environment:get    |
|                                     |                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:application:listApplications    | Grant permission to query all applications.     | List         | application *               | -                                     | cae:application:list   |
| cae:application:createApplication   | Grant permission to create an application.      | Write        | application *               | -                                     | cae:application:create |
|                                     |                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:application:deleteApplication   | Grant permission to delete an application.      | Write        | application *               | -                                     | cae:application:delete |
|                                     |                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:component:listComponents        | Grant permission to query all components.       | List         | component *                 | -                                     | cae:application:list   |
|                                     |                                                 |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |



| Action                                  | Description                                                                                             | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| cae:component:createComponent           | Grant permission to create a component.                                                                 | Write        | component *                 | -                                     | cae:application:create |
|                                         |                                                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:component:deleteComponent           | Grant permission to delete a component.                                                                 | Write        | component *                 | -                                     | cae:application:delete |
|                                         |                                                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:component:updateComponent           | Grant permission to update a component.                                                                 | Write        | component *                 | -                                     | cae:application:modify |
|                                         |                                                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:component:getComponent              | Grant permission to query a component.                                                                  | Read         | component *                 | -                                     | cae:application:get    |
|                                         |                                                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:component:createWithConfigComponent | Grant permission to create, validate, and deploy a component.                                           | Write        | component *                 | -                                     | cae:application:create |
|                                         |                                                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |
| cae:component:operateComponent          | Grant permission to deploy, scale, upgrade, roll back, start, stop, restart, and configure a component. | Write        | component *                 | -                                     | cae:application:modify |
|                                         |                                                                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                        |

| Action                               | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                         |
|--------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------------------------------|
| cae:component:listConfigurations     | Grant permission to query all component configurations.        | List         | component *                 | -                                     | cae:application:get           |
|                                      |                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                               |
| cae:component:createConfiguration    | Grant permission to create or update component configurations. | Write        | component *                 | -                                     | cae:application:create        |
|                                      |                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                               |
| cae:component:deleteConfiguration    | Grant permission to delete or cancel component configurations. | Write        | component *                 | -                                     | cae:application:delete        |
|                                      |                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                               |
| cae:component:getConfiguration       | Grant permission to query component configurations.            | Read         | component *                 | -                                     | cae:application:list          |
|                                      |                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                               |
| cae:component:createInstanceWebShell | Grant permission to create a remote login.                     | Write        | component *                 | -                                     | cae:application:createConsole |
|                                      |                                                                |              | -                           | <a href="#">g:EnterpriseProjectId</a> |                               |
| cae::listNoticeRules                 | Grant permission to query all event notification rules.        | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:get           |

| Action                | Description                                            | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|-----------------------|--------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| cae::createNoticeRule | Grant permission to create an event notification rule. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:create |
| cae::deleteNoticeRule | Grant permission to delete an event notification rule. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:delete |
| cae::updateNoticeRule | Grant permission to update an event notification rule. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:update |
| cae::getNoticeRule    | Grant permission to query an event notification rule.  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:get    |
| cae::listDewSecrets   | Grant permission to query all secrets.                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:get    |
| cae::createDewSecret  | Grant permission to create a secret.                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:create |
| cae::deleteDewSecret  | Grant permission to delete a secret.                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:delete |
| cae::updateDewSecret  | Grant permission to update a secret.                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:update |

| Action            | Description                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                  |
|-------------------|-----------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------|
| cae::getDewSecret | Grant permission to query a secret.                 | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:get    |
| cae::buyPackage   | Grant permission to purchase a pay-per-use package. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | cae:environment:create |

Each API of CAE usually supports one or more actions. [Table 3-229](#) lists the supported actions and dependencies.

**Table 3-229** Actions and dependencies supported by CAE APIs

| API                                                            | Action                            | Dependencies |
|----------------------------------------------------------------|-----------------------------------|--------------|
| GET /v1/{project_id}/cae/environments                          | cae:environment:listEnvironments  | -            |
| POST /v1/{project_id}/cae/environments                         | cae:environment:createEnvironment | -            |
| DELETE /v1/{project_id}/cae/environments/{environment_id}      | cae:environment:deleteEnvironment | -            |
| POST /v1/{project_id}/cae/environments/{environment_id}/wakeup | cae:environment:createEnvironment | -            |
| GET /v1/{project_id}/cae/collections                           | cae:environment:getEnvironment    | -            |
| GET /v1/{project_id}/cae/applications/comb                     | cae:environment:getEnvironment    | -            |

| API                                                       | Action                            | Dependencies |
|-----------------------------------------------------------|-----------------------------------|--------------|
| GET /v1/{project_id}/cae/volumes                          | cae:environment:listCloudVolumes  | -            |
| POST /v1/{project_id}/cae/volumes                         | cae:environment:createCloudVolume | -            |
| DELETE /v1/{project_id}/cae/volumes/{id}                  | cae:environment:deleteCloudVolume | -            |
| GET /v1/{project_id}/cae/domains                          | cae:environment:listDomains       | -            |
| POST /v1/{project_id}/cae/domains                         | cae:environment:createDomain      | -            |
| DELETE /v1/{project_id}/cae/domains/{domain_id}           | cae:environment:deleteDomain      | -            |
| GET /v1/{project_id}/cae/certificates                     | cae:environment:listCertificates  | -            |
| POST /v1/{project_id}/cae/certificates                    | cae:environment:createCertificate | -            |
| PUT /v1/{project_id}/cae/certificates/{certificate_id}    | cae:environment:updateCertificate | -            |
| DELETE /v1/{project_id}/cae/certificates/{certificate_id} | cae:environment:deleteCertificate | -            |
| GET /v1/{project_id}/cae/timer-rules                      | cae:environment:listTimerRules    | -            |
| POST /v1/{project_id}/cae/timer-rules                     | cae:environment:createTimerRule   | -            |

| API                                                                    | Action                           | Dependencies |
|------------------------------------------------------------------------|----------------------------------|--------------|
| DELETE /v1/{project_id}/cae/timer-rules/{timer_rule_id}                | cae:environment:deleteTimerRule  | -            |
| PUT /v1/{project_id}/cae/timer-rules/{timer_rule_id}                   | cae:environment:updateTimerRule  | -            |
| GET /v1/{project_id}/cae/timer-rules/{timer_rule_id}/execution-results | cae:environment:getTimerRule     | -            |
| GET /v1/{project_id}/cae/eips                                          | cae:environment:listEips         | -            |
| PUT /v1/{project_id}/cae/eips                                          | cae:environment:updateEip        | -            |
| GET /v1/{project_id}/cae/vpc-egress                                    | cae:environment:listVpcEgresses  | -            |
| POST /v1/{project_id}/cae/vpc-egress                                   | cae:environment:createVpcEgress  | -            |
| DELETE /v1/{project_id}/cae/vpc-egress/{vpc_egress_id}                 | cae:environment:deleteVpcEgress  | -            |
| GET /v1/{project_id}/cae/vpc-ingress                                   | cae:environment:listVpcIngresses | -            |
| POST /v1/{project_id}/cae/vpc-ingress                                  | cae:environment:createVpcIngress | -            |
| DELETE /v1/{project_id}/cae/vpc-ingress/{vpc_ingress_id}               | cae:environment:deleteVpcIngress | -            |
| GET /v1/{project_id}/cae/monitor-system                                | cae:environment:getMonitorSystem | -            |

| API                                                                              | Action                              | Dependencies |
|----------------------------------------------------------------------------------|-------------------------------------|--------------|
| POST /v1/{project_id}/cae/monitor-system                                         | cae:environment:createMonitorSystem | -            |
| PUT /v1/{project_id}/cae/monitor-system/{monitor_system_id}                      | cae:environment:updateMonitorSystem | -            |
| GET /v1/{project_id}/cae/applications                                            | cae:application:listApplications    | -            |
| POST /v1/{project_id}/cae/applications                                           | cae:application:createApplication   | -            |
| DELETE /v1/{project_id}/cae/applications/{application_id}                        | cae:application:deleteApplication   | -            |
| GET /v1/{project_id}/cae/applications/{application_id}                           | cae:application:listApplications    | -            |
| POST /v1/{project_id}/cae/applications/{application_id}/components               | cae:component:createComponent       | -            |
| GET /v1/{project_id}/cae/applications/{application_id}/components                | cae:component:listComponents        | -            |
| GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id} | cae:component:getComponent          | -            |
| PUT /v1/{project_id}/cae/applications/{application_id}/components/{component_id} | cae:component:updateComponent       | -            |

| API                                                                                                         | Action                            | Dependencies |
|-------------------------------------------------------------------------------------------------------------|-----------------------------------|--------------|
| DELETE /v1/{project_id}/cae/applications/{application_id}/components/{component_id}                         | cae:component:deleteComponent     | -            |
| POST /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/action                    | cae:component:operateComponent    | -            |
| GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configurations             | cae:component:listConfigurations  | -            |
| POST /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configurations            | cae:component:createConfiguration | -            |
| DELETE /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configurations          | cae:component:deleteConfiguration | -            |
| GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configuration-history-time | cae:component:getConfiguration    | -            |



| API                                                                                                           | Action                               | Dependencies |
|---------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/configuration-history        | cae:component:getConfiguration       | -            |
| GET /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/instances                    | cae:component:getComponent           | -            |
| DELETE /v1/{project_id}/cae/applications/{application_id}/components/{component_id}/instances/{instance_name} | cae:component:deleteComponent        | -            |
| POST /v1/{project_id}/cae/remote-console/{instance_id}                                                        | cae:component:createInstanceWebShell | -            |
| GET /v1/{project_id}/cae/jobs/{job_id}                                                                        | cae:environment:getEnvironment       | -            |
| POST /v1/{project_id}/cae/jobs/{job_id}                                                                       | cae:environment:createEnvironment    | -            |
| POST /v1/{project_id}/cae/notice-rules                                                                        | cae::createNoticeRule                | -            |
| GET /v1/{project_id}/cae/notice-rules                                                                         | cae::listNoticeRules                 | -            |
| PUT /v1/{project_id}/cae/notice-rules/{rule_id}                                                               | cae::updateNoticeRule                | -            |

| API                                                                   | Action                        | Dependencies |
|-----------------------------------------------------------------------|-------------------------------|--------------|
| GET /v1/{project_id}/cae/notice-rules/{rule_id}                       | cae::getNoticeRule            | -            |
| DELETE /v1/{project_id}/cae/notice-rules/{rule_id}                    | cae::deleteNoticeRule         | -            |
| POST /v1/{project_id}/cae/dew-secrets                                 | cae::createDewSecret          | -            |
| GET /v1/{project_id}/cae/dew-secrets                                  | cae::listDewSecrets           | -            |
| PUT /v1/{project_id}/cae/dew-secrets/{secret_id}                      | cae::updateDewSecret          | -            |
| DELETE /v1/{project_id}/cae/dew-secrets/{secret_id}                   | cae::deleteDewSecret          | -            |
| GET /v1/{project_id}/cae/dew-secrets/{secret_id}/effective-components | cae::getDewSecret             | -            |
| GET /v1/{project_id}/cae/demo                                         | cae:component:getComponent    | -            |
| POST /v1/{project_id}/cae/demo/install                                | cae:component:createComponent | -            |
| POST /v1/{project_id}/cae/orders                                      | cae::buyPackage               | -            |

## Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in [Table 3-230](#), the resource URN must be specified in the SCP statements using that action, and the SCP applies only to resources of this

type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the SCP applies to all resources. You can also set condition keys in an SCP to define resource types.

The following table lists the resource types that you can define in SCP statements for CAE.

**Table 3-230** Resource types supported by CAE

| Resource Type | URN                                                                 |
|---------------|---------------------------------------------------------------------|
| component     | cae:<region>:<account-id>:component:<application-id>/<component-id> |
| environment   | cae:<region>:<account-id>:environment:<environment-id>              |
| application   | cae:<region>:<account-id>:application:<application-id>              |

## Conditions

cae does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.12 Business Applications

### 3.12.1 Domain Name Service

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by DNS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by DNS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for DNS.

**Table 3-231** Actions supported by DNS

| Action        | Description                          | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------|--------------------------------------|--------------|-----------------------------|---------------|-------|
| dns:zone:list | Grants permission to list the zones. | List         | zone *                      | -             | -     |

| Action                                | Description                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|---------------------------------------|-----------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                       |                                               |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |       |
| dns:zone:create                       | Grants permission to create a zone.           | Write        | zone *                      | -                                                                                                                                                                                      |       |
|                                       |                                               |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |       |
| dns:zone:createBatchPublicZonesByName | Grants permission to create zones in batches. | Write        | zone *                      | -                                                                                                                                                                                      |       |
|                                       |                                               |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |       |
| dns:zone:get                          | Grants permission to obtain a zone.           | Read         | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -     |
| dns:zone:update                       | Grants permission to update a zone.           | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -     |
| dns:zone:delete                       | Grants permission to delete a zone.           | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -     |

| Action                       | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dns:zone:associate-router    | Grants permission to associate a VPC with a private zone.                   | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:zone:disassociate-router | Grants permission to disassociate a VPC from a private zone.                | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:zone:setProxyPattern     | Grants permission to set recursive resolution proxy for private subdomains. | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:zone:transfer            | Grants permission to transfer public domain names.                          | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:recordset:list           | Grants permission to list the record sets.                                  | List         | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:recordset:create         | Grants permission to create a record set.                                   | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-----------------------|-------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                       |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">dns:RecordSetNames</a></li> <li>• <a href="#">dns:RecordSetTypes</a></li> </ul>               |       |
| dns:recordset: get    | Grants permission to obtain a record set. | Read         | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:recordset: update | Grants permission to update a record set. | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                       |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">dns:RecordSetNames</a></li> <li>• <a href="#">dns:RecordSetTypes</a></li> </ul>               |       |
| dns:recordset: delete | Grants permission to delete a record set. | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                       |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">dns:RecordSetNames</a></li> <li>• <a href="#">dns:RecordSetTypes</a></li> </ul>               |       |
| dns:zone:setStatus    | Grants permission to set the zone status. | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                | Description                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|---------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dns:recordset:setStatus               | Grants permission to set the record set status.                     | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                       |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">dns:RecordSetName</a></li> <li>• <a href="#">dns:RecordSetTypes</a></li> </ul>                |       |
| dns:recordset:associatehealthcheck    | Grants permission to associate a record set with a health check.    | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                       |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">dns:RecordSetName</a></li> <li>• <a href="#">dns:RecordSetTypes</a></li> </ul>                |       |
| dns:recordset:disassociatehealthcheck | Grants permission to disassociate a record set from a health check. | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                       |                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">dns:RecordSetName</a></li> <li>• <a href="#">dns:RecordSetTypes</a></li> </ul>                |       |
| dns:ptr:list                          | Grants permission to list the PTR records.                          | List         | ptr *                       | -                                                                                                                                                  | -     |



| Action         | Description                                    | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias         |
|----------------|------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
|                |                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |               |
| dns:ptr:get    | Grants permission to obtain a PTR record.      | Read         | ptr *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | -             |
| dns:ptr:create | Grants permission to create a PTR record.      | Write        | ptr *                       | -                                                                                                                                                                                      | • dns:ptr:set |
|                |                                                |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |               |
| dns:ptr:update | Grants permission to update a PTR record.      | Write        | ptr *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | • dns:ptr:set |
| dns:ptr:delete | Grants permission to delete a PTR record.      | Write        | ptr *                       | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                     | • dns:ptr:set |
| dns:tag:get    | Grants permission to query tags of a resource. | Read         | zone                        | -                                                                                                                                                                                      | -             |
|                |                                                |              | ptr                         | -                                                                                                                                                                                      |               |

| Action                           | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                          |
|----------------------------------|-------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------|
| dns:tag:set                      | Grants permission to one or more tags to a resource.  | Tagging      | zone                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                              |
|                                  |                                                       |              | ptr                         | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                                                |
| dns:zone:createRetrieval         | Grants permission to retrieve a zone.                 | Write        | -                           | -                                             | -                                                              |
| dns:zone:getRetrieval            | Grants permission to query the zone retrieval status. | Read         | -                           | -                                             | -                                                              |
| dns:customLine:create            | Grants permission to create a custom line.            | Write        | customLine *                | -                                             | -                                                              |
| dns:customLine:list              | Grants permission to list the custom lines.           | List         | customLine *                | -                                             | -                                                              |
| dns:customLine:delete            | Grants permission to delete a custom line.            | Write        | customLine *                | -                                             | -                                                              |
| dns:customLine:update            | Grants permission to update a custom line.            | Write        | customLine *                | -                                             | -                                                              |
| dns:nameserver:list              | Grants permission to list the name servers.           | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>dns:zone:get</li> </ul> |
| dns:nameserver:getZoneNameServer | Grants permission to query public DNS servers.        | Read         | -                           | -                                             | -                                                              |

| Action                                          | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                               |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| dns:quota:list                                  | Grants permission to list quotas.                                                             | List         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>dns:zone:get</li> </ul>                      |
| dns:recordset:getPrivateRecordSetImport         | Grants permission to query the import task record sets added to a private zone.               | Read         | zone *                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dns:privateRecordset:getImport</li> </ul>    |
| dns:recordset:getPrivateRecordSetImportTemplate | Grants permission to download the template for importing record sets added to a private zone. | Read         | -                           | -                                                                                                                                              | <ul style="list-style-type: none"> <li>dns:privateRecordset:getImport</li> </ul>    |
| dns:recordset:createPrivateRecordSetImport      | Grants permission to create an import task for record sets added to a private zone.           | Write        | zone *                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dns:privateRecordset:createImport</li> </ul> |
| dns:recordset:deletePrivateRecordSetImportTask  | Grants permission to delete the import task record sets added to a private zone.              | Write        | zone *                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dns:privateRecordset:deleteImport</li> </ul> |
| dns:recordset:createPublicRecordSetImport       | Grants permission to create an import task for record sets added to a public zone.            | Write        | zone *                      | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>dns:publicRecordset:createImport</li> </ul>  |

| Action                                         | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                              |
|------------------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| dns:recordset:getPublicRecordSetImport         | Grants permission to query the import task for record sets added to a public zone.           | Read         | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dns:publicRecordset:getImport    |
| dns:recordset:getPublicRecordSetImportTemplate | Grants permission to download the template for importing record sets added to a public zone. | Read         | -                           | -                                                                                                                                                  | • dns:publicRecordset:getImport    |
| dns:recordset:deletePublicRecordSetImportTask  | Grants permission to delete the import task for record sets added to a public zone.          | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | • dns:publicRecordset:deleteImport |
| dns:zone:getExport                             | Grants permission to export zones.                                                           | Read         | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                  |
| dns:lineGroup:create                           | Grants permission to create a line group.                                                    | Write        | lineGroup *                 | -                                                                                                                                                  | -                                  |
| dns:lineGroup:list                             | Grants permission to list the line groups.                                                   | List         | lineGroup *                 | -                                                                                                                                                  | -                                  |
| dns:lineGroup:get                              | Grants permission to query a line group.                                                     | Read         | lineGroup *                 | -                                                                                                                                                  | -                                  |

| Action                       | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dns:lineGroup:delete         | Grants permission to delete a line group.                                  | Write        | lineGroup *                 | -             | -     |
| dns:lineGroup:update         | Grants permission to update a line group.                                  | Write        | lineGroup *                 | -             | -     |
| dns:endpoint:create          | Grants permission to create a resolver endpoint.                           | Write        | endpoint *                  | -             | -     |
| dns:endpoint:list            | Grants permission to list the resolver endpoints.                          | List         | endpoint *                  | -             | -     |
| dns:endpoint:get             | Grants permission to query a specified resolver endpoint.                  | Read         | endpoint *                  | -             | -     |
| dns:endpoint:update          | Grants permission to update a resolver endpoint.                           | Write        | endpoint *                  | -             | -     |
| dns:endpoint:delete          | Grants permission to delete a resolver endpoint.                           | Write        | endpoint *                  | -             | -     |
| dns:endpoint:createIpaddress | Grants permission to bind a specified IP address with a resolver endpoint. | Write        | endpoint *                  | -             | -     |

| Action                         | Description                                                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------|--------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| dns:endpoint:deletelpaddresses | Grants permission to unbind a specified IP address from a resolver endpoint.                           | Write        | endpoint *                  | -             | -     |
| dns:endpoint:listlppaddresses  | Grants permission to list the IP addresses bound to a resolver endpoint.                               | List         | endpoint *                  | -             | -     |
| dns:endpoint:listVpcs          | Grants permission to list the VPCs associated with a resolver endpoint.                                | List         | endpoint *                  | -             | -     |
| dns:resolverRule:create        | Grants permission to create a resolver rule to route queries originating from your VPC out of the VPC. | Write        | resolverRule *              | -             | -     |
| dns:resolverRule:list          | Grants permission to list the resolver rules.                                                          | List         | resolverRule *              | -             | -     |
| dns:resolverRule:get           | Grants permission to query a resolver rule.                                                            | Read         | resolverRule *              | -             | -     |

| Action                              | Description                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias |
|-------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| dns:resolverRule:update             | Grants permission to update a resolver rule.                             | Write        | resolverRule *              | -                                                                                                                                                  | -     |
| dns:resolverRule:delete             | Grants permission to delete a resolver rule.                             | Write        | resolverRule *              | -                                                                                                                                                  | -     |
| dns:resolverRule:associateRouter    | Grants permission to associate a resolver rule with a VPC.               | Write        | resolverRule *              | -                                                                                                                                                  | -     |
| dns:resolverRule:disassociateRouter | Grants permission to disassociate a resolver rule from a VPC.            | Write        | resolverRule *              | -                                                                                                                                                  | -     |
| dns:zone:enableDnssecConfig         | Grants permission to enable the DNSSEC configuration for a public zone.  | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:zone:disableDnssecConfig        | Grants permission to disable the DNSSEC configuration for a public zone. | Write        | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
| dns:zone:getDnssecConfig            | Grants permission to query the DNSSEC configuration from a public zone.  | Read         | zone *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |

| Action                                        | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                  | Alias                                                               |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| dns:zone:listPublicZoneBatchOperationRecords  | Grants permission to list batch operations of public zones.                                     | List         | -                           | -                                                                                                              | <ul style="list-style-type: none"> <li>dns:recordset:get</li> </ul> |
| dns:zone:getPublicZoneBatchOperationResult    | Grants permission to download the public zones that failed to be operated in a batch operation. | Read         | -                           | -                                                                                                              | <ul style="list-style-type: none"> <li>dns:recordset:get</li> </ul> |
| dns:recordset:batchImportPublicRecordSet      | Grants permission to import record sets added to public zones.                                  | Write        | -                           | -                                                                                                              | -                                                                   |
| dns:zone:createAuthorizeTxtRecord             | Grants permission to authorize a zone.                                                          | Write        | -                           | -                                                                                                              | -                                                                   |
| dns:zone:getAuthorizeTxtRecord                | Grants permission to query the zone authorization status.                                       | Read         | -                           | -                                                                                                              | -                                                                   |
| dns:zone:getDomainDetection                   | Grants permission to query the detection result of a public zone record set.                    | Read         | zone *                      | <ul style="list-style-type: none"> <li>g:ResourceTag/&lt;tag-key&gt;</li> <li>g:EnterpriseProjectId</li> </ul> | -                                                                   |
| dns:recordset:batchDeletePublicZoneRecordsets | Grants permission to delete public zone record sets in batches.                                 | Write        | -                           | -                                                                                                              | -                                                                   |



| Action                                        | Description                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                      |
|-----------------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------------------------------------------------|
| dns:recordset:batchUpdatePublicZoneRecordsets | Grants permission to update public zone record sets in batches. | Write        | -                           | -             | -                                                                                          |
| dns:recordset:batchCreatePublicZoneRecordsets | Grants permission to create public zone record sets in batches. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>dns:recordset:batchImportPublicRecordSet</li> </ul> |

Each API of DNS usually supports one or more actions. [Table 3-232](#) lists the supported actions and dependencies.

**Table 3-232** Actions and dependencies supported by DNS APIs

| API                                    | Action          | Dependencies                                                                                                                                                                                 |
|----------------------------------------|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET 01 /v2/zones                       | dns:zone:list   | -                                                                                                                                                                                            |
| POST 05 /v2/zones                      | dns:zone:create | <ul style="list-style-type: none"> <li>dns:tag:set</li> <li>dns:quota:list</li> </ul>                                                                                                        |
| GET 01 /v2/zones/{zone_id}             | dns:zone:get    | -                                                                                                                                                                                            |
| PATCH 03 /v2/zones/{zone_id}           | dns:zone:update | -                                                                                                                                                                                            |
| DELETE 02 /v2/zones/{zone_id}          | dns:zone:delete | <ul style="list-style-type: none"> <li>ces:siteMonitorRule:showHealthCheck</li> <li>ces:siteMonitorRule:put</li> <li>ces:siteMonitorRule:delete</li> <li>ces:siteMonitorRule:list</li> </ul> |
| GET 01 /v2/zones/{zone_id}/nameservers | dns:zone:get    | -                                                                                                                                                                                            |
| GET /v2/zones                          | dns:zone:list   | -                                                                                                                                                                                            |

| API                                                | Action                      | Dependencies                                                                                                                                                                                                                                                     |
|----------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST 02 /v2/zones                                  | dns:zone:create             | <ul style="list-style-type: none"> <li>vpc:vpcs:get</li> <li>dns:tag:set</li> <li>dns:quota:list</li> </ul>                                                                                                                                                      |
| GET 04 /v2/zones/{zone_id}                         | dns:zone:get                | -                                                                                                                                                                                                                                                                |
| PATCH 06 /v2/zones/{zone_id}                       | dns:zone:update             | -                                                                                                                                                                                                                                                                |
| DELETE 05 /v2/zones/{zone_id}                      | dns:zone:delete             | <ul style="list-style-type: none"> <li>ces:siteMonitorRule:showHealthCheck</li> <li>ces:siteMonitorRule:put</li> <li>ces:siteMonitorRule:delete</li> <li>ces:siteMonitorRule:list</li> </ul>                                                                     |
| GET /v2/zones/{zone_id}/nameservers                | dns:zone:get                | -                                                                                                                                                                                                                                                                |
| POST /v2/zones/{zone_id}/associaterouter           | dns:zone:associaterouter    | vpc:vpcs:get                                                                                                                                                                                                                                                     |
| POST /v2/zones/{zone_id}/disassociaterouter        | dns:zone:disassociaterouter | vpc:vpcs:get                                                                                                                                                                                                                                                     |
| POST /v2/zones/{zone_id}/actions/set-proxy-pattern | dns:zone:setProxyPattern    | -                                                                                                                                                                                                                                                                |
| GET /v2/zones/{zone_id}/recordsets                 | dns:recordset:list          | -                                                                                                                                                                                                                                                                |
| POST /v2/zones/{zone_id}/recordsets                | dns:recordset:create        | <ul style="list-style-type: none"> <li>dns:recordset:associatehealthcheck</li> <li>ces:siteMonitorRule:showHealthCheck</li> <li>ces:siteMonitorRule:put</li> <li>ces:siteMonitorRule:delete</li> <li>ces:siteMonitorRule:list</li> <li>dns:quota:list</li> </ul> |
| GET /v2/zones/{zone_id}/recordsets/{recordset_id}  | dns:recordset:get           | -                                                                                                                                                                                                                                                                |

| API                                                     | Action               | Dependencies                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT 02 /v2/zones/{zone_id}/recordsets/{recordset_id}    | dns:recordset:update | -                                                                                                                                                                                                                                                                            |
| DELETE 01 /v2/zones/{zone_id}/recordsets/{recordset_id} | dns:recordset:delete | <ul style="list-style-type: none"> <li>• dns:recordset:disassociatehealthcheck</li> <li>• ces:siteMonitorRule:showHealthCheck</li> <li>• ces:siteMonitorRule:put</li> <li>• ces:siteMonitorRule:delete</li> <li>• ces:siteMonitorRule:list</li> </ul>                        |
| GET /v2/recordsets                                      | dns:recordset:list   | -                                                                                                                                                                                                                                                                            |
| PUT /v2/zones/{zone_id}/statuses                        | dns:zone:setStatus   | -                                                                                                                                                                                                                                                                            |
| GET /v2.1/recordsets                                    | dns:recordset:list   | -                                                                                                                                                                                                                                                                            |
| POST /v2.1/zones/{zone_id}/recordsets                   | dns:recordset:create | <ul style="list-style-type: none"> <li>• dns:recordset:associatehealthcheck</li> <li>• ces:siteMonitorRule:showHealthCheck</li> <li>• ces:siteMonitorRule:put</li> <li>• ces:siteMonitorRule:delete</li> <li>• ces:siteMonitorRule:list</li> <li>• dns:quota:list</li> </ul> |
| GET 03 /v2.1/zones/{zone_id}/recordsets                 | dns:recordset:list   | -                                                                                                                                                                                                                                                                            |
| GET 01 /v2.1/zones/{zone_id}/recordsets/{recordset_id}  | dns:recordset:get    | -                                                                                                                                                                                                                                                                            |
| PUT 03 /v2.1/zones/{zone_id}/recordsets/{recordset_id}  | dns:recordset:update | -                                                                                                                                                                                                                                                                            |

| API                                                       | Action                  | Dependencies                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE 02 /v2.1/zones/{zone_id}/recordsets/{recordset_id} | dns:recordset:delete    | <ul style="list-style-type: none"> <li>• dns:recordset:disassociatehealthcheck</li> <li>• ces:siteMonitorRule:showHealthCheck</li> <li>• ces:siteMonitorRule:put</li> <li>• ces:siteMonitorRule:delete</li> <li>• ces:siteMonitorRule:list</li> </ul>                        |
| PUT /v2.1/recordsets/{recordset_id}/statuses/set          | dns:recordset:setStatus | -                                                                                                                                                                                                                                                                            |
| POST /v2.1/zones/{zone_id}/recordsets/batch/lines         | dns:recordset:create    | <ul style="list-style-type: none"> <li>• dns:recordset:associatehealthcheck</li> <li>• ces:siteMonitorRule:showHealthCheck</li> <li>• ces:siteMonitorRule:put</li> <li>• ces:siteMonitorRule:delete</li> <li>• ces:siteMonitorRule:list</li> <li>• dns:quota:list</li> </ul> |
| PUT /v2.1/zones/{zone_id}/recordsets                      | dns:recordset:update    | -                                                                                                                                                                                                                                                                            |
| DELETE /v2.1/zones/{zone_id}/recordsets                   | dns:recordset:delete    | <ul style="list-style-type: none"> <li>• dns:recordset:disassociatehealthcheck</li> <li>• ces:siteMonitorRule:showHealthCheck</li> <li>• ces:siteMonitorRule:put</li> <li>• ces:siteMonitorRule:delete</li> <li>• ces:siteMonitorRule:list</li> </ul>                        |
| GET /v2/reverse/floatingips                               | dns:ptr:list            | -                                                                                                                                                                                                                                                                            |
| GET 02 /v2/reverse/floatingips/{region}:{floatingip_id}   | dns:ptr:get             | -                                                                                                                                                                                                                                                                            |
| PATCH 01 /v2/reverse/floatingips/{region}:{floatingip_id} | dns:ptr:create          | <ul style="list-style-type: none"> <li>• dns:tag:set</li> <li>• eip:publicips:get</li> <li>• dns:quota:list</li> </ul>                                                                                                                                                       |

| API                                                        | Action                  | Dependencies                                                                                                                                                                                                                                          |
|------------------------------------------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PATCH 04 /v2/reverse/floatingips/{region}:{floatingip_id}  | dns:ptr:update          | -                                                                                                                                                                                                                                                     |
| PATCH 03 /v2/reverse/floatingips/{region}:{floatingip_id}  | dns:ptr:delete          | -                                                                                                                                                                                                                                                     |
| DELETE /v2.1/zones                                         | dns:zone:delete         | <ul style="list-style-type: none"> <li>• ces:siteMonitorRule:showHealthCheck</li> <li>• ces:siteMonitorRule:put</li> <li>• ces:siteMonitorRule:delete</li> <li>• ces:siteMonitorRule:list</li> </ul>                                                  |
| DELETE /v2.1/reverse/floatingips                           | dns:ptr:delete          | -                                                                                                                                                                                                                                                     |
| PUT /v2.1/zones/statuses                                   | dns:zone:setStatus      | -                                                                                                                                                                                                                                                     |
| PUT /v2.1/recordsets/statuses                              | dns:recordset:setStatus | -                                                                                                                                                                                                                                                     |
| DELETE 02 /v2.1/recordsets                                 | dns:recordset:delete    | <ul style="list-style-type: none"> <li>• dns:recordset:disassociatehealthcheck</li> <li>• ces:siteMonitorRule:showHealthCheck</li> <li>• ces:siteMonitorRule:put</li> <li>• ces:siteMonitorRule:delete</li> <li>• ces:siteMonitorRule:list</li> </ul> |
| GET /v2/{project_id}/{resource_type}/tags                  | dns:tag:get             | -                                                                                                                                                                                                                                                     |
| GET 02 /v2/{project_id}/{resource_type}/{resource_id}/tags | dns:tag:get             | -                                                                                                                                                                                                                                                     |
| POST /v2/{project_id}/{resource_type}/{resource_id}/tags   | dns:tag:set             | -                                                                                                                                                                                                                                                     |

| API                                                              | Action                | Dependencies                                                                                                                                        |
|------------------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/{key} | dns:tag:set           | -                                                                                                                                                   |
| POST /v2/{project_id}/{resource_type}/{resource_id}/tags/action  | dns:tag:set           | -                                                                                                                                                   |
| POST /v2/{project_id}/{resource_type}/resource_instances/action  | dns:tag:get           | -                                                                                                                                                   |
| POST /v2.1/customlines                                           | dns:customLine:create | dns:quota:list                                                                                                                                      |
| GET /v2.1/customlines                                            | dns:customLine:list   | -                                                                                                                                                   |
| DELETE /v2.1/customlines/{line_id}                               | dns:customLine:delete | -                                                                                                                                                   |
| PUT /v2.1/customlines/{line_id}                                  | dns:customLine:update | -                                                                                                                                                   |
| GET /v2/nameservers                                              | dns:nameserver:list   | -                                                                                                                                                   |
| GET /v2/quotamg/dns/quotas                                       | dns:quota:list        | -                                                                                                                                                   |
| POST /v2.1/endpoints                                             | dns:endpoint:create   | <ul style="list-style-type: none"> <li>• vpc:subnets:get</li> <li>• vpc:networks:get</li> <li>• vpc:ports:list</li> <li>• dns:quota:list</li> </ul> |
| GET /v2.1/endpoints                                              | dns:endpoint:list     | -                                                                                                                                                   |
| GET /v2.1/endpoints/{endpoint_id}                                | dns:endpoint:get      | -                                                                                                                                                   |
| PUT /v2.1/endpoints/{endpoint_id}                                | dns:endpoint:update   | -                                                                                                                                                   |

| API                                                             | Action                              | Dependencies                                                                                                        |
|-----------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| DELETE /v2.1/endpoints/{endpoint_id}                            | dns:endpoint:delete                 | <ul style="list-style-type: none"> <li>vpc:ports:list</li> <li>vpc:ports:delete</li> </ul>                          |
| POST /v2.1/endpoints/{endpoint_id}/ipaddresses                  | dns:endpoint:createipaddresses      | <ul style="list-style-type: none"> <li>vpc:subnets:get</li> <li>vpc:networks:get</li> <li>vpc:ports:list</li> </ul> |
| GET /v2.1/endpoints/{endpoint_id}/ipaddresses                   | dns:endpoint:listipaddresses        | -                                                                                                                   |
| DELETE /v2.1/endpoints/{endpoint_id}/ipaddresses/{ipaddress_id} | dns:endpoint:deleteipaddresses      | <ul style="list-style-type: none"> <li>vpc:ports:list</li> <li>vpc:ports:delete</li> </ul>                          |
| GET /v2.1/vpcs                                                  | dns:endpoint:listVpcs               | -                                                                                                                   |
| POST /v2.1/resolverrules                                        | dns:resolverRule:create             | -                                                                                                                   |
| GET /v2.1/resolverrules                                         | dns:resolverRule:list               | -                                                                                                                   |
| POST /v2.1/resolverrules/{resolverrule_id}/associaterouter      | dns:resolverRule:associaterouter    | vpc:vpcs:get                                                                                                        |
| POST /v2.1/resolverrules/{resolverrule_id}/disassociaterouter   | dns:resolverRule:disassociaterouter | -                                                                                                                   |
| GET /v2.1/resolverrules/{resolverrule_id}                       | dns:resolverRule:get                | -                                                                                                                   |
| PUT /v2.1/resolverrules/{resolverrule_id}                       | dns:resolverRule:update             | -                                                                                                                   |
| DELETE /v2.1/resolverrules/{resolverrule_id}                    | dns:resolverRule:delete             | -                                                                                                                   |
| POST /v2.1/linegroups                                           | dns:lineGroup:create                | dns:quota:list                                                                                                      |

| API                                      | Action                            | Dependencies |
|------------------------------------------|-----------------------------------|--------------|
| GET /v2.1/linegroups                     | dns:lineGroup:list                | -            |
| GET /v2.1/linegroups/{linegroup_id}      | dns:lineGroup:get                 | -            |
| PUT /v2.1/linegroups/{linegroup_id}      | dns:lineGroup:update              | -            |
| DELETE /v2.1/linegroups/{linegroup_id}   | dns:lineGroup:delete              | -            |
| POST /v2/zones/{zone_id}/enable-dnssec   | dns:zone:enableDnssecConfig       | -            |
| POST /v2/zones/{zone_id}/disable-dnssec  | dns:zone:disableDnssecConfig      | -            |
| GET /v2/zones/{zone_id}/dnssec           | dns:zone:getDnssecConfig          | -            |
| POST /v2/authorize-txtrecord             | dns:zone:createAuthorizeTxtRecord | -            |
| GET /v2/authorize-txtrecord              | dns:zone:getAuthorizeTxtRecord    | -            |
| POST /v2/authorize-txtrecord/{id}/verify | dns:zone:createAuthorizeTxtRecord | -            |
| PUT /v2.1/ptrs/{ptr_id}                  | dns:ptr:update                    | -            |
| DELETE /v2.1/ptrs/{ptr_id}               | dns:ptr:delete                    | -            |
| POST /v2.1/ptrs                          | dns:ptr:create                    | -            |
| GET /v2.1/ptrs                           | dns:ptr:list                      | -            |
| GET /v2.1/ptrs/{ptr_id}                  | dns:ptr:get                       | -            |
| GET /v2.1/zones/{zone_id}/lines          | dns:zone:get                      | -            |
| PUT 02 /v2/zones/{zone_id}/statuses      | dns:zone:setStatus                | -            |



## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-233](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for DNS.

**Table 3-233** Resource types supported by DNS

| Resource Type | URN                                                       |
|---------------|-----------------------------------------------------------|
| resolverRule  | dns:<region>:<account-id>:resolverRule:<resolver-rule-id> |
| lineGroup     | dns::<account-id>:lineGroup:<line-group-id>               |
| customLine    | dns::<account-id>:customLine:<custom-line-id>             |
| zone          | dns::<account-id>:zone:<zone-id>                          |
| endpoint      | dns:<region>:<account-id>:endpoint:<endpoint-id>          |
| ptr           | dns:<region>:<account-id>:ptr:<ptr-id>                    |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, dns) apply only to operations of the xx service. For details, see [Table 3-234](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple

tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.

- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by DNS

The following table lists the condition keys that you can define in identity policies for DNS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-234** Service-specific condition keys supported by DNS

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                                      |
|--------------------------------|--------|-------------------------------|------------------------------------------------------------------------------------------------------------------|
| dns:RecordSetNames             | string | Multivalued                   | Filters access by record set name. The name can contain only lowercase letters and cannot have the trailing dot. |
| dns:RecordSetTypes             | string | Multivalued                   | Filters access by record set type. The type can be A, AAAA, MX, CNAME, TXT, NS, SRV or CAA.                      |

## 3.13 Media Services

### 3.13.1 Live (Live)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by Live, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Live, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Live.

**Table 3-235** Actions supported by Live

| Action                                | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:domain:createDomain              | Grants permission to create a domain name.                                           | Write        | -                           | -             | -     |
| live:domain:getDomains                | Grants permission to query a domain name.                                            | Read         | -                           | -             | -     |
| live:domain:deleteDomain              | Grants permission to delete a domain name.                                           | Write        | -                           | -             | -     |
| live:domain:updateDomain              | Grants permission to modify a domain name.                                           | Write        | -                           | -             | -     |
| live:domain:createDomains Mapping     | Grants permission to map domain names.                                               | Write        | -                           | -             | -     |
| live:domain:deleteDomains Mapping     | Grants permission to delete the mapping between domain names.                        | Write        | -                           | -             | -     |
| live:domain:updateStream Notification | Grants permission to add or modify the configuration of stream status notifications. | Write        | -                           | -             | -     |

| Action                               | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:domain:getStreamNotifications   | Grants permission to query the configuration of stream status notifications.  | Read         | -                           | -             | -     |
| live:domain:deleteStreamNotification | Grants permission to delete the configuration of stream status notifications. | Write        | -                           | -             | -     |
| live:domain:createCDNConfig          | Grants permission to create domain name configuration items.                  | Write        | -                           | -             | -     |
| live:domain:updateCDNConfig          | Grants permission to modify domain name configuration items.                  | Write        | -                           | -             | -     |
| live:domain:getCDNConfig             | Grants permission to query domain name configuration items.                   | Read         | -                           | -             | -     |
| live:domain:deleteCDNConfig          | Grants permission to delete domain name configuration items.                  | Write        | -                           | -             | -     |

| Action                         | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:domain:getIPAuthList      | Grants permission to query the IP address blacklist or whitelist.           | Read         | -                           | -             | -     |
| live:domain:updateIPAuthList   | Grants permission to modify the IP address blacklist or whitelist.          | Write        | -                           | -             | -     |
| live:domain:getGeoBlockingList | Grants permission to obtain regions with livestreaming restrictions.        | Read         | -                           | -             | -     |
| live:domain:updateGeoBlocking  | Grants permission to modify regions with livestreaming restrictions.        | Write        | -                           | -             | -     |
| live:domain:updateRefererChain | Grants permission to set the referer validation blacklist and whitelist.    | Write        | -                           | -             | -     |
| live:domain:deleteRefererChain | Grants permission to delete the referer validation blacklist and whitelist. | Write        | -                           | -             | -     |

| Action                      | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:domain:getRefererChain | Grants permission to query the referer validation blacklist and whitelist. | Read         | -                           | -             | -     |
| live:logs:listLog           | Grants permission to obtain the link for downloading playback logs.        | Read         | -                           | -             | -     |
| live:domain:getCertificates | Grants permission to query HTTPS certificate information.                  | Read         | -                           | -             | -     |
| live:record:createRule      | Grants permission to create a recording rule.                              | Write        | -                           | -             | -     |
| live:record:listRules       | Grants permission to query recording rules.                                | Read         | -                           | -             | -     |
| live:record:updateRule      | Grants permission to modify a recording rule.                              | Write        | -                           | -             | -     |
| live:record:deleteRule      | Grants permission to delete a recording rule.                              | Write        | -                           | -             | -     |

| Action                     | Description                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:record:getRule        | Grants permission to query a recording rule.                     | Read         | -                           | -             | -     |
| live:record:listContents   | Grants permission to query recordings.                           | Read         | -                           | -             | -     |
| live:record:createCommand  | Grants permission to submit a command for controlling recording. | Write        | -                           | -             | -     |
| live:record:createCallback | Grants permission to create a recording callback rule.           | Write        | -                           | -             | -     |
| live:record:listCallbacks  | Grants permission to query recording callback rules.             | Read         | -                           | -             | -     |
| live:record:updateCallback | Grants permission to modify a recording callback rule.           | Write        | -                           | -             | -     |
| live:record:getCallback    | Grants permission to query a recording callback rule.            | Read         | -                           | -             | -     |
| live:record:deleteCallback | Grants permission to delete a recording callback rule.           | Write        | -                           | -             | -     |



| Action                            | Description                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:snapshot:createRule          | Grants permission to configure snapshot capture.                | Write        | -                           | -             | -     |
| live:snapshot:updateRule          | Grants permission to modify snapshot capture.                   | Write        | -                           | -             | -     |
| live:snapshot:listRules           | Grants permission to query snapshot capture.                    | Read         | -                           | -             | -     |
| live:snapshot:deleteRule          | Grants permission to delete snapshot capture.                   | Write        | -                           | -             | -     |
| live:stream:createStreamForbidden | Grants permission to disable a push stream.                     | Write        | -                           | -             | -     |
| live:stream:listStreamForbidden   | Grants permission to query disabled streams.                    | Read         | -                           | -             | -     |
| live:stream:deleteStreamForbidden | Grants permission to resume a push stream.                      | Write        | -                           | -             | -     |
| live:stream:updateStreamForbidden | Grants permission to modify the attribute of a disabled stream. | Write        | -                           | -             | -     |

| Action                                | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:stream:createStreamForbiddenOnce | Grants permission to disconnect a stream.                                        | Write        | -                           | -             | -     |
| live:stream:listLiveStreamsOnline     | Grants permission to query online streams.                                       | Read         | -                           | -             | -     |
| live:stream:createPullTask            | Grants permission to create a task for ingesting streams from external networks. | Write        | -                           | -             | -     |
| live:stream:deletePullTask            | Grants permission to delete a task for ingesting streams from external networks. | Write        | -                           | -             | -     |
| live:stream:listPullTask              | Grants permission to query a task for ingesting streams from external networks.  | Read         | -                           | -             | -     |
| live:tenant:updateChargingMode        | Grants permission to configure the billing mode.                                 | Write        | -                           | -             | -     |
| live:tenant:getTenantInformation      | Grants permission to query tenant information.                                   | Read         | -                           | -             | -     |

| Action                                    | Description                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------------------|-----------------------------------------------------|--------------|-----------------------------|---------------|-------|
| live:transcode:createTranscodingsTemplate | Grants permission to create a transcoding template. | Write        | -                           | -             | -     |
| live:transcode:deleteTranscodingsTemplate | Grants permission to delete a transcoding template. | Write        | -                           | -             | -     |
| live:transcode:updateTranscodingsTemplate | Grants permission to modify a transcoding template. | Write        | -                           | -             | -     |
| live:transcode:listTranscodingTemplate    | Grants permission to query a transcoding template.  | Read         | -                           | -             | -     |
| live:transcode:createSEI                  | Grants permission to add transcoding SEI.           | Write        | -                           | -             | -     |

Each API of Live usually supports one or more actions. [Table 3-236](#) lists the supported actions and dependencies.

**Table 3-236** Actions and dependencies supported by Live APIs

| API                            | Action                   | Dependencies |
|--------------------------------|--------------------------|--------------|
| POST /v1/{project_id}/domain   | live:domain:createDomain | -            |
| DELETE /v1/{project_id}/domain | live:domain:deleteDomain | -            |
| PUT /v1/{project_id}/domain    | live:domain:updateDomain | -            |

| API                                           | Action                                | Dependencies |
|-----------------------------------------------|---------------------------------------|--------------|
| GET /v1/{project_id}/domain                   | live:domain:getDomains                | -            |
| PUT /v1/{project_id}/domains_mapping          | live:domain:createDomains Mapping     | -            |
| DELETE /v1/{project_id}/domains_mapping       | live:domain:deleteDomains Mapping     | -            |
| PUT /v1/{project_id}/notifications/publish    | live:domain:updateStreamN otification | -            |
| GET /v1/{project_id}/notifications/publish    | live:domain:getStreamNotif ications   | -            |
| DELETE /v1/{project_id}/notifications/publish | live:domain:deleteStreamN otification | -            |
| POST /v1/{project_id}/domain/config           | live:domain:createCDNConfi g          | -            |
| PUT /v1/{project_id}/domain/config            | live:domain:updateCDNConf ig          | -            |
| GET /v1/{project_id}/domain/config            | live:domain:getCDNConfig              | -            |
| DELETE /v1/{project_id}/domain/config         | live:domain:deleteCDNConf ig          | -            |
| GET /v1/{project_id}/guard/ip                 | live:domain:getIPAuthList             | -            |
| PUT /v1/{project_id}/guard/ip                 | live:domain:updateIPAuthLi st         | -            |
| GET /v1/{project_id}/guard/geo-blocking       | live:domain:getGeoBlocking List       | -            |
| PUT /v1/{project_id}/guard/geo-blocking       | live:domain:updateGeoBloc king        | -            |

| API                                         | Action                         | Dependencies |
|---------------------------------------------|--------------------------------|--------------|
| PUT /v1/{project_id}/guard/referer-chain    | live:domain:updateRefererChain | -            |
| DELETE /v1/{project_id}/guard/referer-chain | live:domain:deleteRefererChain | -            |
| GET /v1/{project_id}/guard/referer-chain    | live:domain:getRefererChain    | -            |
| GET /v1/{project_id}/logs                   | live:logs:listLog              | -            |
| GET /v2/{project_id}/certificates           | live:domain:getCertificates    | -            |
| POST /v1/{project_id}/record/rules          | live:record:createRule         | -            |
| GET /v1/{project_id}/record/rules           | live:record:listRules          | -            |
| PUT /v1/{project_id}/record/rules/{id}      | live:record:updateRule         | -            |
| DELETE /v1/{project_id}/record/rules/{id}   | live:record:deleteRule         | -            |
| GET /v1/{project_id}/record/rules/{id}      | live:record:getRule            | -            |
| GET /v1/{project_id}/record/contents        | live:record:listContents       | -            |
| POST /v1/{project_id}/record/control        | live:record:createCommand      | -            |
| POST /v1/{project_id}/record/callbacks      | live:record:createCallback     | -            |
| GET /v1/{project_id}/record/callbacks       | live:record:listCallbacks      | -            |

| API                                           | Action                                | Dependencies |
|-----------------------------------------------|---------------------------------------|--------------|
| PUT /v1/{project_id}/record/callbacks/{id}    | live:record:updateCallback            | -            |
| GET /v1/{project_id}/record/callbacks/{id}    | live:record:getCallback               | -            |
| DELETE /v1/{project_id}/record/callbacks/{id} | live:record:deleteCallback            | -            |
| POST /v1/{project_id}/stream/snapshot         | live:snapshot:createRule              | -            |
| PUT /v1/{project_id}/stream/snapshot          | live:snapshot:updateRule              | -            |
| GET /v1/{project_id}/stream/snapshot          | live:snapshot:listRules               | -            |
| DELETE /v1/{project_id}/stream/snapshot       | live:snapshot:deleteRule              | -            |
| POST /v1/{project_id}/stream/blocks           | live:stream:createStreamForbidden     | -            |
| GET /v1/{project_id}/stream/blocks            | live:stream:listStreamForbidden       | -            |
| DELETE /v1/{project_id}/stream/blocks         | live:stream:deleteStreamForbidden     | -            |
| PUT /v1/{project_id}/stream/blocks            | live:stream:updateStreamForbidden     | -            |
| POST /v1/{project_id}/stream/block-once       | live:stream:createStreamForbiddenOnce | -            |
| GET /v1/{project_id}/realtime/streams         | live:stream:listLiveStreamsOnline     | -            |

| API                                           | Action                                    | Dependencies |
|-----------------------------------------------|-------------------------------------------|--------------|
| POST /v1/{project_id}/pull/stream             | live:stream:createPullTask                | -            |
| DELETE /v1/{project_id}/pull/stream           | live:stream:deletePullTask                | -            |
| GET /v1/{project_id}/pull/stream_list         | live:stream:listPullTask                  | -            |
| PUT /v1/{project_id}/tenant/charging_mode     | live:tenant:updateCharging Mode           | -            |
| GET /v1/{project_id}/tenant/info              | live:tenant:getTenantInformation          | -            |
| POST /v1/{project_id}/template/transcodings   | live:transcode:createTranscodingsTemplate | -            |
| DELETE /v1/{project_id}/template/transcodings | live:transcode:deleteTranscodingsTemplate | -            |
| PUT /v1/{project_id}/template/transcodings    | live:transcode:updateTranscodingsTemplate | -            |
| GET /v1/{project_id}/template/transcodings    | live:transcode:listTranscodingsTemplate   | -            |
| PUT /v1/{project_id}/transcode/sei            | live:transcode:createSEI                  | -            |
| GET /v1/{project_id}/guard/key-chain          | live:domain:getCDNConfig                  | -            |
| PUT /v1/{project_id}/guard/key-chain          | live:domain:updateCDNConfig               | -            |

| API                                      | Action                      | Dependencies |
|------------------------------------------|-----------------------------|--------------|
| DELETE /v1/{project_id}/guard/key-chain  | live:domain:deleteCDNConfig | -            |
| PUT /v1/{project_id}/guard/https-cert    | live:domain:updateCDNConfig | -            |
| GET /v1/{project_id}/guard/https-cert    | live:domain:getCDNConfig    | -            |
| DELETE /v1/{project_id}/guard/https-cert | live:domain:deleteCDNConfig | -            |
| POST /v1/{project_id}/pull/stream/task   | live:stream:createPullTask  | -            |
| DELETE /v1/{project_id}/pull/stream/task | live:stream:deletePullTask  | -            |
| GET /v1/{project_id}/pull/stream/task    | live:stream:listPullTask    | -            |

## Resources

Live does not support resource-level authorization. To allow access to Live, use a wildcard (\*) in the Resource element of the identity policy, indicating that the identity policy will be applied to all resources.

## Conditions

Live does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.13.2 Media Processing Center (MPC)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that



OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by MPC, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by MPC, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for MPC.

**Table 3-237** Actions supported by MPC

| Action                       | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| mpc:transcodeTemplate:create | Grants permission to create a transcoding template.                        | Write        | -                           | -             | -     |
| mpc:transcodeTemplate:update | Grants permission to modify a custom transcoding template.                 | Write        | -                           | -             | -     |
| mpc:transcodeTemplate:delete | Grants permission to delete a custom transcoding template.                 | Write        | -                           | -             | -     |
| mpc:transcodeTemplate:view   | Grants permission to queries one or more custom transcoding templates.     | List         | -                           | -             | -     |
| mpc:templateGroup:create     | Grants permission to create a transcoding template group.                  | Write        | -                           | -             | -     |
| mpc:templateGroup:view       | Grants permission to query one or more custom transcoding template groups. | Write        | -                           | -             | -     |

| Action                       | Description                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| mpc:templateGroup:update     | Grants permission to modify a custom transcoding template group.   | Write        | -                           | -             | -     |
| mpc:templateGroup:delete     | Grants permission to delete a custom transcoding template group.   | Write        | -                           | -             | -     |
| mpc:watermarkTemplate:create | Grants permission to Create a custom watermark template.           | Write        | -                           | -             | -     |
| mpc:watermarkTemplate:update | Grants permission to modify a watermark template.                  | Write        | -                           | -             | -     |
| mpc:watermarkTemplate:delete | Grants permission to delete a watermark template.                  | Write        | -                           | -             | -     |
| mpc:watermarkTemplate:view   | Grants permission to query one or more custom watermark templates. | List         | -                           | -             | -     |
| mpc:transcodeTask:create     | Grants permission to create a transcoding task.                    | Write        | -                           | -             | -     |

| Action                                  | Description                                               | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| mpc:transcodeTask:delete                | Grants permission to cancel a transcoding task.           | Write        | -                           | -             | -     |
| mpc:transcodeTask:view                  | Grants permission to query one or more transcoding tasks. | Read         | -                           | -             | -     |
| mpc:transcodeTask:deleteRecord          | Grants permission to delete transcoding task records.     | Write        | -                           | -             | -     |
| mpc:transcodeTask:viewSummaryStatistics | Grants permission to query the task duration statistics.  | List         | -                           | -             | -     |
| mpc:remuxTask:create                    | Grants permission to create a packaging task.             | Write        | -                           | -             | -     |
| mpc:remuxTask:retry                     | Grants permission to retry a failed packaging task.       | Write        | -                           | -             | -     |
| mpc:remuxTask:view                      | Grants permission to query one or more packaging tasks.   | List         | -                           | -             | -     |

| Action                          | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| mpc:remuxTask:delete            | Grants permission to cancel a packaging task.                                         | Write        | -                           | -             | -     |
| mpc:remuxTask:deleteRecord      | Grants permission to delete packaging task records.                                   | Write        | -                           | -             | -     |
| mpc:animatedGraphicsTask:create | Grants permission to create an animated GIF task.                                     | Write        | -                           | -             | -     |
| mpc:animatedGraphicsTask:view   | Grants permission to query one or more animated GIF tasks.                            | List         | -                           | -             | -     |
| mpc:animatedGraphicsTask:delete | Grants permission to cancel an animated GIF task.                                     | Write        | -                           | -             | -     |
| mpc:extractTask:create          | Grants permission to create a task to parse the metadata of a video file.             | Write        | -                           | -             | -     |
| mpc:extractTask:view            | Grants permission to query the status and results of one or more video parsing tasks. | List         | -                           | -             | -     |

| Action                    | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| mpc:extractTask:delete    | Grants permission to cancel a video parsing task.                             | Write        | -                           | -             | -     |
| mpc:thumbnailsTask:view   | Grants permission to query one or more snapshot tasks.                        | List         | -                           | -             | -     |
| mpc:thumbnailsTask:delete | Grants permission to cancel a snapshot task.                                  | Write        | -                           | -             | -     |
| mpc:notification:config   | Grants permission to configure event notifications on the transcoding server. | Write        | -                           | -             | -     |
| mpc:notification:view     | Grants permission to query the enabling statuses of subscription events.      | List         | -                           | -             | -     |
| mpc:notifyEvent:view      | Grants permission to query all subscription events of an SMN topic.           | List         | -                           | -             | -     |
| mpc:bucket:view           | Grants permission to query the list of buckets in a specified region.         | List         | -                           | -             | -     |

| Action                      | Description                                                                             | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| mpc:bucket:updateAuthorized | Grants permission to authorizes MPC to access OBS buckets or cancels the authorization. | Write        | -                           | -             | -     |
| mpc:bucketObject:view       | Grants permission to queries objects in a bucket.                                       | List         | -                           | -             | -     |
| mpc:agencyTask:create       | Grants permission to enables or disables OBS Authorization.                             | Write        | -                           | -             | -     |
| mpc:agencyTask:view         | Grants permission to queries the status of creating an OBS authorization task.          | Read         | -                           | -             | -     |

Each API of MPC usually supports one or more actions. [Table 3-238](#) lists the supported actions and dependencies.

**Table 3-238** Actions and dependencies supported by MPC APIs

| API                                         | Action                       | Dependencies |
|---------------------------------------------|------------------------------|--------------|
| POST /v1/{project_id}/template/transcodings | mpc:transcodeTemplate:create | -            |
| PUT /v1/{project_id}/template/transcodings  | mpc:transcodeTemplate:update | -            |

| API                                                 | Action                       | Dependencies |
|-----------------------------------------------------|------------------------------|--------------|
| DELETE /v1/{project_id}/template/transcodings       | mpc:transcodeTemplate:delete | -            |
| GET /v1/{project_id}/template/transcodings          | mpc:transcodeTemplate:view   | -            |
| POST /v1/{project_id}/template_group/transcodings   | mpc:templateGroup:create     | -            |
| GET /v1/{project_id}/template_group/transcodings    | mpc:templateGroup:view       | -            |
| PUT /v1/{project_id}/template_group/transcodings    | mpc:templateGroup:update     | -            |
| DELETE /v1/{project_id}/template_group/transcodings | mpc:templateGroup:delete     | -            |
| POST /v1/{project_id}/template/watermark            | mpc:watermarkTemplate:create | -            |
| PUT /v1/{project_id}/template/watermark             | mpc:watermarkTemplate:update | -            |
| DELETE /v1/{project_id}/template/watermark          | mpc:watermarkTemplate:delete | -            |
| GET /v1/{project_id}/template/watermark             | mpc:watermarkTemplate:view   | -            |
| POST /v1/{project_id}/transcodings                  | mpc:transcodeTask:create     | -            |



| API                                         | Action                                  | Dependencies |
|---------------------------------------------|-----------------------------------------|--------------|
| DELETE /v1/{project_id}/transcodings        | mpc:transcodeTask:delete                | -            |
| GET /v1/{project_id}/transcodings           | mpc:transcodeTask:view                  | -            |
| DELETE /v1/{project_id}/transcodings/task   | mpc:transcodeTask:deleteRecord          | -            |
| GET /v1/{project_id}/transcodings/summaries | mpc:transcodeTask:viewSummaryStatistics | -            |
| POST /v1/{project_id}/remux                 | mpc:remuxTsk:create                     | -            |
| PUT /v1/{project_id}/remux                  | mpc:remuxTsk:retry                      | -            |
| GET /v1/{project_id}/remux                  | mpc:remuxTsk:view                       | -            |
| DELETE /v1/{project_id}/remux               | mpc:remuxTsk:delete                     | -            |
| DELETE /v1/{project_id}/remux/task          | mpc:remuxTsk:deleteRecord               | -            |
| POST /v1/{project_id}/animated-graphics     | mpc:animatedGraphicsTask:create         | -            |
| GET /v1/{project_id}/animated-graphics      | mpc:animatedGraphicsTask:view           | -            |
| DELETE /v1/{project_id}/animated-graphics   | mpc:animatedGraphicsTask:delete         | -            |
| POST /v1/{project_id}/extract-metadata      | mpc:extractTask:create                  | -            |
| GET /v1/{project_id}/extract-metadata       | mpc:extractTask:view                    | -            |

| API                                      | Action                      | Dependencies |
|------------------------------------------|-----------------------------|--------------|
| DELETE /v1/{project_id}/extract-metadata | mpc:extracTask:delete       | -            |
| POST /v1/{project_id}/thumbnails         | mpc:thumbnailsTask:create   | -            |
| GET /v1/{project_id}/thumbnails          | mpc:thumbnailsTask:view     | -            |
| DELETE /v1/{project_id}/thumbnails       | mpc:thumbnailsTask:delete   | -            |
| PUT /v1/{project_id}/notification        | mpc:notification:config     | -            |
| GET /v1/{project_id}/notification        | mpc:notification:view       | -            |
| GET /v1/{project_id}/notification/event  | mpc:notifyEvent:view        | -            |
| GET /v1/{project_id}/buckets             | mpc:bucket:view             | -            |
| PUT /v1/{project_id}/authority           | mpc:bucket:updateAuthorized | -            |
| GET /v1.0-ext/{project_id}/objects       | mpc:bucketObject:view       | -            |
| POST /v1/{project_id}/agencies           | mpc:agenciesTask:create     | -            |
| GET /v1/{project_id}/agencies            | mpc:agenciesTask:view       | -            |

## Resources

MPC does not support resource-level authorization. To allow access to MPC, use a wildcard (\*) in the Resource element of the identity policy, indicating that the identity policy will be applied to all resources.

## Conditions

MPC does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.14 Management & Governance

### 3.14.1 Identity and Access Management (IAM)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by IAM, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by IAM, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for IAM.

**Table 3-239** Actions supported by IAM

| Action               | Description                                         | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                |
|----------------------|-----------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------------------------------------------|
| iam::listAccessKeys  | Grants permission to list permanent access keys.    | List         | -                           | -             | <ul style="list-style-type: none"> <li>• iam:credentials:listCredentials</li> </ul>  |
| iam::createAccessKey | Grants permission to create a permanent access key. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>• iam:credentials:createCredential</li> </ul> |
| iam::getAccessKey    | Grants permission to query a permanent access key.  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>• iam:credentials:getCredential</li> </ul>    |
| iam::updateAccessKey | Grants permission to update a permanent access key. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>• iam:credentials:updateCredential</li> </ul> |

| Action                   | Description                                             | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                              |
|--------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------|
| iam::deleteAccessKey     | Grants permission to delete a permanent access key.     | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:credentials:deleteCredential</li> </ul> |
| iam:projects:list        | Grants permission to list projects.                     | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:projects:listProjects</li> </ul>        |
| iam:projects:create      | Grants permission to create a project.                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:projects:createProject</li> </ul>       |
| iam:projects:listForUser | Grants permission to list projects of a specified user. | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:projects:listProjectsForUser</li> </ul> |
| iam:projects:update      | Grants permission to update a project.                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:projects:updateProject</li> </ul>       |
| iam:groups:list          | Grants permission to list groups.                       | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:groups:listGroups</li> </ul>            |
| iam:groups:create        | Grants permission to create a group.                    | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:groups:createGroup</li> </ul>           |
| iam:groups:get           | Grants permission to query a group.                     | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:groups:getGroup</li> </ul>              |
| iam:groups:delete        | Grants permission to delete a group.                    | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:groups:deleteGroup</li> </ul>           |

| Action                | Description                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                 |
|-----------------------|------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------------|
| iam:groups:update     | Grants permission to update a group.                       | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:groups:updateGroup</li> </ul>              |
| iam:groups:removeUser | Grants permission to remove user from a group.             | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:removeUserFromGroup</li> </ul> |
| iam:groups:listUsers  | Grants permission to list users of a specified group.      | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:listUsersForGroup</li> </ul>         |
| iam:groups:checkUser  | Grants permission to query whether a user is in the group. | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:checkUserInGroup</li> </ul>    |
| iam:groups:addUser    | Grants permission to add user to a group.                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:addUserToGroup</li> </ul>      |
| iam:users:create      | Grants permission to create a user.                        | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:createUser</li> </ul>                |
| iam:users:get         | Grants permission to query a user.                         | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:getUser</li> </ul>                   |
| iam:users:update      | Grants permission to update a user.                        | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:updateUser</li> </ul>                |
| iam:users:list        | Grants permission to list users.                           | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:listUsers</li> </ul>                 |
| iam:users:delete      | Grants permission to delete a user.                        | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:deleteUser</li> </ul>                |

| Action                           | Description                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                         |
|----------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------------------|
| iam:users:listGroups             | Grants permission to list groups of a specified user.              | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:groups:listGroupsForUser</li> </ul>                |
| iam:users:listVirtualMFADevices  | Grants permission to list virtual MFA devices of a specified user. | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:mfa:listVirtualMFADevices</li> </ul>               |
| iam:users:createVirtualMFADevice | Grants permission to create a virtual MFA device.                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:mfa:createVirtualMFADevice</li> </ul>              |
| iam:users:deleteVirtualMFADevice | Grants permission to delete a virtual MFA device.                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:mfa:deleteVirtualMFADevice</li> </ul>              |
| iam:users:getVirtualMFADevice    | Grants permission to query a virtual MFA device.                   | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:mfa:getVirtualMFADevice</li> </ul>                 |
| iam:users:bindVirtualMFADevice   | Grants permission to bind a virtual MFA device.                    | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:mfa:bindMFADevice</li> </ul>                       |
| iam:users:unbindVirtualMFADevice | Grants permission to unbind a virtual MFA device.                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:mfa:unbindMFADevice</li> </ul>                     |
| iam:identityProviders:list       | Grants permission to list identity providers.                      | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:listIdentityProviders</li> </ul> |

| Action                              | Description                                                  | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                          |
|-------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------------------|
| iam:identityProviders:get           | Grants permission to query an identity provider.             | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:getIdentityProvider</li> </ul>    |
| iam:identityProviders:create        | Grants permission to create an identity provider.            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:createIdentityProvider</li> </ul> |
| iam:identityProviders:delete        | Grants permission to delete an identity provider.            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:deleteIdentityProvider</li> </ul> |
| iam:identityProviders:update        | Grants permission to update an identity provider.            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:updateIdentityProvider</li> </ul> |
| iam:identityProviders:listMappings  | Grants permission to list mappings of an identity provider.  | List         | -                           | -             | -                                                                                              |
| iam:identityProviders:getMapping    | Grants permission to query mapping of an identity provider.  | Read         | -                           | -             | -                                                                                              |
| iam:identityProviders:createMapping | Grants permission to create mapping of an identity provider. | Write        | -                           | -             | -                                                                                              |



| Action                               | Description                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| iam:identityProviders:deleteMapping  | Grants permission to delete mapping of an identity provider.    | Write        | -                           | -             | -     |
| iam:identityProviders:updateMapping  | Grants permission to update mapping of an identity provider.    | Write        | -                           | -             | -     |
| iam:identityProviders:listProtocols  | Grants permission to list protocols of an identity provider.    | List         | -                           | -             | -     |
| iam:identityProviders:getProtocol    | Grants permission to query protocol of an identity provider.    | Read         | -                           | -             | -     |
| iam:identityProviders:createProtocol | Grants permission to create protocol of an identity provider.   | Write        | -                           | -             | -     |
| iam:identityProviders:deleteProtocol | Grants permission to delete protocol of an identity provider.   | Write        | -                           | -             | -     |
| iam:identityProviders:updateProtocol | Grants permission to update a protocol of an identity provider. | Write        | -                           | -             | -     |

| Action                                   | Description                                                             | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                             |
|------------------------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------------------------|
| iam:identityProviders:getSAMLMetadata    | Grants permission to query SAML metadata file of an identity provider.  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:getIDPMetadata</li> </ul>            |
| iam:identityProviders:createSAMLMetadata | Grants permission to create SAML metadata file of an identity provider. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:createIDPMetadata</li> </ul>         |
| iam:identityProviders:getOIDCConfig      | Grants permission to query OIDC configuration of an identity provider.  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:getOpenIDConnectConfig</li> </ul>    |
| iam:identityProviders:createOIDCConfig   | Grants permission to create OIDC configuration of an identity provider. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:createOpenIDConnectConfig</li> </ul> |
| iam:identityProviders:updateOIDCConfig   | Grants permission to update OIDC configuration of an identity provider. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:identityProviders:updateOpenIDConnectConfig</li> </ul> |
| iam:securityPolicies:getProtectPolicy    | Grants permission to query an operation protection policy.              | Read         | -                           | -             | -                                                                                                 |

| Action                                      | Description                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| iam:securityPolicies:updateProtectPolicy    | Grants permission to update an operation protection policy. | Write        | -                           | -             | -     |
| iam:securityPolicies:getPasswordPolicy      | Grants permission to query a password policy.               | Read         | -                           | -             | -     |
| iam:securityPolicies:updatePasswordPolicy   | Grants permission to update a password policy.              | Write        | -                           | -             | -     |
| iam:securityPolicies:getLoginPolicy         | Grants permission to query a login policy.                  | Read         | -                           | -             | -     |
| iam:securityPolicies:updateLoginPolicy      | Grants permission to update a login policy.                 | Write        | -                           | -             | -     |
| iam:securityPolicies:getConsoleAclPolicy    | Grants permission to query a console access policy.         | Read         | -                           | -             | -     |
| iam:securityPolicies:updateConsoleAclPolicy | Grants permission to modify a console access policy.        | Write        | -                           | -             | -     |
| iam:securityPolicies:getApiAclPolicy        | Grants permission to query an API access policy.            | Read         | -                           | -             | -     |

| Action                                           | Description                                                          | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                             |
|--------------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------|
| iam:securityPolicies:updateApiAclPolicy          | Grants permission to update an API access policy.                    | Write        | -                           | -             | -                                                                                 |
| iam:securityPolicies:getPrivacyTransferPolicy    | Grants permission to query a privacy transfer policy.                | Read         | -                           | -             | -                                                                                 |
| iam:securityPolicies:updatePrivacyTransferPolicy | Grants permission to update a privacy transfer policy.               | Write        | -                           | -             | -                                                                                 |
| iam:users:listLoginProtectSettings               | Grants permission to list user login protect settings of the domain. | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:listUserLoginProtects</li> </ul> |
| iam:users:getLoginProtectSetting                 | Grants permission to get the login protect setting.                  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:getUserLoginProtect</li> </ul>   |
| iam:users:updateLoginProtectSetting              | Grants permission to update the login protect setting.               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:users:setUserLoginProtect</li> </ul>   |
| iam:quotas:list                                  | Grants permission to list quotas.                                    | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:quotas:listQuotas</li> </ul>           |
| iam:quotas:listForProject                        | Grants permission to list quotas of a specified project.             | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:quotas:listQuotasForProject</li> </ul> |

| Action                        | Description                                                            | Access Level          | Resource Type (*: required) | Condition Key | Alias                                                                                        |
|-------------------------------|------------------------------------------------------------------------|-----------------------|-----------------------------|---------------|----------------------------------------------------------------------------------------------|
| iam:agencies:pass             | Grants permission to pass an agency to a service.                      | Permission management | agency *                    | -             | -                                                                                            |
| iam:roles:list                | Grants permission to list roles.                                       | List                  | -                           | -             | <ul style="list-style-type: none"> <li>iam:roles:listRoles</li> </ul>                        |
| iam:roles:get                 | Grants permission to get role detail.                                  | Read                  | -                           | -             | <ul style="list-style-type: none"> <li>iam:roles:getRole</li> </ul>                          |
| iam::listRoleAssignments      | Grants permission to query tenant assignment records.                  | List                  | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRoleAssignments</li> </ul>        |
| iam:groups:listRolesOnDomain  | Grants permission to query user group permissions in global services.  | List                  | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForGroupOnDomain</li> </ul>  |
| iam:groups:listRolesOnProject | Grants permission to query user group permissions in project services. | List                  | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForGroupOnProject</li> </ul> |
| iam:groups:grantRoleOnDomain  | Grants permission to grant global service permissions to a user group. | Write                 | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToGroupOnDomain</li> </ul>   |

| Action                        | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                        |
|-------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------------------------|
| iam:groups:grantRoleOnProject | Grants permission to grant project level service to a user group.                   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToGroupOnProject</li> </ul>  |
| iam:groups:checkRoleOnDomain  | Grants permission to query whether a user group has global service permissions.     | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:checkRoleForGroupOnDomain</li> </ul>  |
| iam:groups:checkRoleOnProject | Grants permission to query whether a user group has the project service permission. | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:checkRoleForGroupOnProject</li> </ul> |
| iam:groups:listRoles          | Grants permission to query permissions of a user group.                             | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForGroup</li> </ul>          |
| iam:groups:checkRole          | Grants permission to query whether a user group has specified permissions.          | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:checkRoleForGroup</li> </ul>          |
| iam:groups:revokeRole         | Grants permission to remove specified permissions from a user group.                | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromGroup</li> </ul>        |

| Action                                 | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                          |
|----------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------------------|
| iam:groups:revokeRoleOnDomain          | Grants permission to remove global service permissions from a user group.  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromGroupOnDomain</li> </ul>  |
| iam:groups:revokeRoleOnProject         | Grants permission to remove project service permissions from a user group. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromGroupOnProject</li> </ul> |
| iam:groups:grantRole                   | Grants permission to grant specified permissions to a user group.          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToGroup</li> </ul>             |
| iam:roles:create                       | Grants permission to create custom policies.                               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:roles:createRole</li> </ul>                         |
| iam:roles:update                       | Grants permission to create custom policies.                               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:roles:updateRole</li> </ul>                         |
| iam:roles:delete                       | Grants permission to delete custom policies.                               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:roles:deleteRole</li> </ul>                         |
| iam:agencies:list                      | Grants permission to list agencies.                                        | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:agencies:listAgencies</li> </ul>                    |
| iam:agencies:listSwitchAgencyHistories | Grants permission to list the history of switching agency.                 | List         | -                           | -             | -                                                                                              |

| Action                          | Description                                                          | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                         |
|---------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------------------|
| iam:agencies:get                | Grants permission to query agency details.                           | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:agencies:getAgency</li> </ul>                      |
| iam:agencies:create             | Grants permission to create agency.                                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:agencies:createAgency</li> </ul>                   |
| iam:agencies:update             | Grants permission to modify agency.                                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:agencies:updateAgency</li> </ul>                   |
| iam:agencies:delete             | Grants permission to delete agency.                                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:agencies:deleteAgency</li> </ul>                   |
| iam:agencies:listRolesOnDomain  | Grants permission to query global service permissions of an agency.  | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForAgencyOnDomain</li> </ul>  |
| iam:agencies:listRolesOnProject | Grants permission to query project permissions of an agency.         | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForAgencyOnProject</li> </ul> |
| iam:agencies:grantRoleOnDomain  | Grants permission to grant global service permissions to agencies.   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToAgencyOnDomain</li> </ul>   |
| iam:agencies:grantRoleOnProject | Grants permission to grant project services permissions to agencies. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToAgencyOnProject</li> </ul>  |



| Action                           | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------------------------------------------------------------------|
| iam:agencies:checkRoleOnDomain   | Grants permission to query whether an agency has global service permissions.  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:checkRoleForAgencyOnDomain</li> </ul>    |
| iam:agencies:checkRoleOnProject  | Grants permission to query whether an agency has project service permissions. | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:checkRoleForAgencyOnProject</li> </ul>   |
| iam:agencies:revokeRoleOnDomain  | Grants permission to remove agency global service permissions.                | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromAgencyOnDomain</li> </ul>  |
| iam:agencies:revokeRoleOnProject | Grants permission to remove agency project service permissions.               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromAgencyOnProject</li> </ul> |
| iam:agencies:listRoles           | Grants permission to list permissions of agency.                              | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForAgency</li> </ul>            |
| iam:agencies:grantRole           | Grants permission to grant the specified permissions to an agency.            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToAgency</li> </ul>             |

| Action                                   | Description                                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                  |
|------------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------------------------------------------------------------|
| iam:agencies:checkRole                   | Grants permission to check whether an agency has specified permissions.                       | Read         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:checkRoleForAgency</li> </ul>                   |
| iam:agencies:revokeRole                  | Grants permission to remove specified permissions of an agency.                               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromAgency</li> </ul>                 |
| iam::listGroupsAssignedEnterpriseProject | Grants permission to query permissions of a user group associated with an enterprise project. | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listGroupsOnEnterpriseProject</li> </ul>        |
| iam:groups:listRolesOnEnterpriseProject  | Grants permission to query permissions of a user group associated with an enterprise project. | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForGroupOnEnterpriseProject</li> </ul> |
| iam:groups:grantRoleOnEnterpriseProject  | Grants permission to grant permissions to a user group associated with an enterprise project. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToGroupOnEnterpriseProject</li> </ul>  |

| Action                                    | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                    |
|-------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------------------------------------|
| iam:groups:revokeRoleOnEnterpriseProject  | Grants permission to delete permissions of a user group associated with an enterprise project.   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromGroupOnEnterpriseProject</li> </ul> |
| iam:groups:listAssignedEnterpriseProjects | Grants permission to query enterprise projects of group.                                         | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listEnterpriseProjectsForGroup</li> </ul>         |
| iam:users:listAssignedEnterpriseProjects  | Grants permission to query enterprise projects of user.                                          | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listEnterpriseProjectsForUser</li> </ul>          |
| iam::listUsersAssignedEnterpriseProject   | Grants permission to query users directly associated with an enterprise project.                 | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listUsersForEnterpriseProject</li> </ul>          |
| iam:users:listRolesOnEnterpriseProject    | Grants permission to query permissions of a user directly associated with an enterprise project. | List         | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:listRolesForUserOnEnterpriseProject</li> </ul>    |

| Action                                     | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                     |
|--------------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------------------------------|
| iam:users:grantRoleOnEnterpriseProject     | Grants permission to grant permissions to an enterprise project based on users.                   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToUserOnEnterpriseProject</li> </ul>      |
| iam:users:revokeRoleOnEnterpriseProject    | Grants permission to delete permissions of a user directly associated with an enterprise project. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromUserOnEnterpriseProject</li> </ul>   |
| iam:agencies:grantRoleOnEnterpriseProject  | Grants permission to grant permissions to an enterprise project based on agencies.                | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:grantRoleToAgencyOnEnterpriseProject</li> </ul>    |
| iam:agencies:revokeRoleOnEnterpriseProject | Grants permission to delete permissions of an agency associated with an enterprise project.       | Write        | -                           | -             | <ul style="list-style-type: none"> <li>iam:permissions:revokeRoleFromAgencyOnEnterpriseProject</li> </ul> |
| iam:mfa:listMFADevicesV5                   | Grants permission to list MFA devices.                                                            | List         | mfa *                       | -             | -                                                                                                         |

| Action                                      | Description                                                          | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| iam:mfa:createVirtualMFADeviceV5            | Grants permission to create a virtual MFA device.                    | Write        | mfa *                       | -             | -     |
| iam:mfa:deleteVirtualMFADeviceV5            | Grants permission to delete a virtual MFA device.                    | Write        | mfa *                       | -             | -     |
| iam:mfa:enableV5                            | Grants permission to enable a MFA device.                            | Write        | mfa *                       | -             | -     |
| iam:mfa:disableV5                           | Grants permission to disable a MFA device.                           | Write        | mfa *                       | -             | -     |
| iam:securitypolicies:getPasswordPolicyV5    | Grants permission to retrieve information about the password policy. | Read         | -                           | -             | -     |
| iam:securitypolicies:updatePasswordPolicyV5 | Grants permission to update the password policy.                     | Write        | -                           | -             | -     |
| iam:securitypolicies:getLoginPolicyV5       | Grants permission to retrieve information about the login policy.    | Read         | -                           | -             | -     |
| iam:securitypolicies:updateLoginPolicyV5    | Grants permission to update the login policy.                        | Write        | -                           | -             | -     |

| Action                                  | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|-----------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| iam:credentials:listCredentialsV5       | Grants permission to list permanent access keys for an IAM user.                             | List         | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:credentials:showAccessKeyLastUsedV5 | Grants permission to retrieve information about when the specified access key was last used. | Read         | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:credentials:createCredentialV5      | Grants permission to create a permanent access key for an IAM user.                          | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:credentials:updateCredentialV5      | Grants permission to update a permanent access key for an IAM user.                          | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:credentials:deleteCredentialV5      | Grants permission to delete a permanent access key for an IAM user.                          | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:users:changePasswordV5              | Grants permission to an IAM user to change own password.                                     | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                         | Description                                                                                    | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|--------------------------------|------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| iam:users:showLoginProfileV5   | Grants permission to retrieve information about the login profile of an IAM user.              | Read         | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:users:createLoginProfileV5 | Grants permission to create login profile for an IAM user.                                     | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:users:updateLoginProfileV5 | Grants permission to update login profile for an IAM user.                                     | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:users:deleteLoginProfileV5 | Grants permission to delete login profile for an IAM user.                                     | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:users:listUsersV5          | Grants permission to list IAM users.                                                           | List         | user *                      | -                                             | -     |
| iam:users:getUserV5            | Grants permission to retrieve information about an IAM user.                                   | Read         | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:users:showUserLastLoginV5  | Grants permission to retrieve information about when the specified IAM user key was logged in. | Read         | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                           | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|----------------------------------|----------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| iam:users:createUserV5           | Grants permission to create an IAM user.                 | Write        | user *                      | -                                             | -     |
| iam:users:updateUserV5           | Grants permission to update an IAM user.                 | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:users:deleteUserV5           | Grants permission to delete an IAM user.                 | Write        | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:groups:listGroupsV5          | Grants permission to list groups.                        | List         | group *                     | -                                             | -     |
| iam:groups:getGroupV5            | Grants permission to retrieve information about a group. | Read         | group *                     | -                                             | -     |
| iam:groups:createGroupV5         | Grants permission to create a group.                     | Write        | group *                     | -                                             | -     |
| iam:groups:updateGroupV5         | Grants permission to update a group.                     | Write        | group *                     | -                                             | -     |
| iam:groups:deleteGroupV5         | Grants permission to delete a group.                     | Write        | group *                     | -                                             | -     |
| iam:permissions:addUserToGroupV5 | Grants permission to add an IAM user to a group.         | Write        | group *                     | -                                             | -     |



| Action                                | Description                                                                      | Access Level          | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------|----------------------------------------------------------------------------------|-----------------------|-----------------------------|---------------|-------|
| iam:permissions:removeUserFromGroupV5 | Grants permission to remove an IAM user from a group.                            | Write                 | group*                      | -             | -     |
| iam:policies:listV5                   | Grants permission to list identity policies.                                     | List                  | policy*                     | -             | -     |
| iam:policies:getV5                    | Grants permission to retrieve information about an identity policy.              | Read                  | policy*                     | -             | -     |
| iam:policies:createV5                 | Grants permission to create a custom identity policy.                            | Permission_management | policy*                     | -             | -     |
| iam:policies:deleteV5                 | Grants permission to delete a custom identity policy.                            | Permission_management | policy*                     | -             | -     |
| iam:policies:listVersionsV5           | Grants permission to list versions for an identity policy.                       | List                  | policy*                     | -             | -     |
| iam:policies:getVersionV5             | Grants permission to retrieve information about a version of an identity policy. | Read                  | policy*                     | -             | -     |

| Action                           | Description                                                                    | Access Level          | Resource Type (*: required) | Condition Key                                 | Alias |
|----------------------------------|--------------------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------|-------|
| iam:policies:createVersionV5     | Grants permission to create a new version for a custom identity policy.        | Permission_management | policy *                    | -                                             | -     |
| iam:policies:deleteVersionV5     | Grants permission to delete a version for a custom identity policy.            | Permission_management | policy *                    | -                                             | -     |
| iam:policies:setDefaultVersionV5 | Grants permission to set default version for a custom identity policy.         | Permission_management | policy *                    | -                                             | -     |
| iam:agencies:attachPolicyV5      | Grants permission to attach an identity policy to an agency or a trust agency. | Permission_management | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                  |                                                                                |                       | -                           | <a href="#">iam:PolicyURN</a>                 |       |
| iam:groups:attachPolicyV5        | Grants permission to attach an identity policy to a group.                     | Permission_management | group *                     | -                                             | -     |
|                                  |                                                                                |                       | -                           | <a href="#">iam:PolicyURN</a>                 |       |
| iam:users:attachPolicyV5         | Grants permission to attach an identity policy to an IAM user.                 | Permission_management | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                  |                                                                                |                       | -                           | <a href="#">iam:PolicyURN</a>                 |       |

| Action                              | Description                                                                           | Access Level          | Resource Type (*: required) | Condition Key                                 | Alias |
|-------------------------------------|---------------------------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------|-------|
| iam:agencies:detachPolicyV5         | Grants permission to detach an identity policy from an agency or a trust agency.      | Permission_management | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                     |                                                                                       |                       | -                           | <a href="#">iam:PolicyURN</a>                 |       |
| iam:groups:detachPolicyV5           | Grants permission to detach an identity policy from a group.                          | Permission_management | group *                     | -                                             | -     |
|                                     |                                                                                       |                       | -                           | <a href="#">iam:PolicyURN</a>                 |       |
| iam:users:detachPolicyV5            | Grants permission to detach an identity policy from an IAM user.                      | Permission_management | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                     |                                                                                       |                       | -                           | <a href="#">iam:PolicyURN</a>                 |       |
| iam:policies:listEntitiesV5         | Grants permission to list attached entities for an identity policy.                   | List                  | policy *                    | -                                             | -     |
| iam:agencies:listAttachedPoliciesV5 | Grants permission to list attached identity policies for an agency or a trust agency. | List                  | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:groups:listAttachedPoliciesV5   | Grants permission to list attached identity policies for a group.                     | List                  | group *                     | -                                             | -     |

| Action                                              | Description                                                                                                        | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| iam:users:listAttachedPoliciesV5                    | Grants permission to list attached identity policies for an IAM user.                                              | List         | user *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| iam:agencies:createServiceLinkedAgencyV5            | Grants permission to create a service linked agency that allows a cloud service to perform actions on your behalf. | Write        | agency *                    | -                                             | -     |
|                                                     |                                                                                                                    |              | -                           | <a href="#">iam:ServicePrincipal</a>          |       |
| iam:agencies:deleteServiceLinkedAgencyV5            | Grants permission to delete a service linked agency.                                                               | Write        | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                                     |                                                                                                                    |              | -                           | <a href="#">iam:ServicePrincipal</a>          |       |
| iam:agencies:getServiceLinkedAgencyDeletionStatusV5 | Grants permission to retrieve deletion status of a service linked agency.                                          | Read         | agency *                    | -                                             | -     |
| iam:agencies:listV5                                 | Grants permission to list agencies and trust agencies.                                                             | List         | agency *                    | -                                             | -     |
| iam:agencies:getV5                                  | Grants permission to retrieve information about an agency or a trust agency.                                       | Read         | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                           | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|----------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| iam:agencies:createV5            | Grants permission to create a trust agency.                     | Write        | agency *                    | -                                                                                                                                 | -     |
| iam:agencies:updateV5            | Grants permission to update a trust agency.                     | Write        | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| iam:agencies:deleteV5            | Grants permission to delete a trust agency.                     | Write        | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| iam:agencies:updateTrustPolicyV5 | Grants permission to update the trust policy of a trust agency. | Write        | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| iam::listTagsForResourceV5       | Grants permission to list tags for a resource.                  | List         | agency                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                  |                                                                 |              | user                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
| iam::tagForResourceV5            | Grants permission to tag a resource.                            | Tagging      | agency                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                  |                                                                 |              | user                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                                  |                                                                 |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| iam::untagForResourceV5          | Grants permission to untag a resource.                          | Tagging      | agency                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                  |                                                                 |              | user                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |

| Action                              | Description                                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|-------------------------------------|-----------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                     |                                                                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| iam::getAccountSummaryV5            | Grants permission to retrieve information about IAM entity usage and IAM quotas in the IAM account. | List         | -                           | -                                                                                                                                     | -     |
| iam::getAsymmetricSignatureSwitchV5 | Grants permission to query asymmetric signature switch status of security token.                    | Read         | -                           | -                                                                                                                                     | -     |
| iam::setAsymmetricSignatureSwitchV5 | Grants permission to set asymmetric signature switch status of security token.                      | Write        | -                           | -                                                                                                                                     | -     |

Each API of IAM usually supports one or more actions. [Table 3-240](#) lists the supported actions and dependencies.

**Table 3-240** Actions and dependencies supported by IAM APIs

| API                                 | Action              | Dependencies |
|-------------------------------------|---------------------|--------------|
| GET /v3.0/OS-CREDENTIAL/credentials | iam::listAccessKeys | -            |

| API                                                 | Action                    | Dependencies |
|-----------------------------------------------------|---------------------------|--------------|
| POST /v3.0/OS-CREDENTIAL/credentials                | iam::createAccessKey      | -            |
| GET /v3.0/OS-CREDENTIAL/credentials/{access_key}    | iam::getAccessKey         | -            |
| PUT /v3.0/OS-CREDENTIAL/credentials/{access_key}    | iam::updateAccessKey      | -            |
| DELETE /v3.0/OS-CREDENTIAL/credentials/{access_key} | iam::deleteAccessKey      | -            |
| GET /v3.0/OS-QUOTA/domains/{domain_id}              | iam:quotas:list           | -            |
| GET /v3.0/OS-QUOTA/projects/{project_id}            | iam:quotas:listForProject | -            |
| GET /v3/projects                                    | iam:projects:list         | -            |
| POST /v3/projects                                   | iam:projects:create       | -            |
| GET /v3/users/{user_id}/projects                    | iam:projects:listForUser  | -            |
| PATCH /v3/projects/{project_id}                     | iam:projects:update       | -            |
| PUT /v3-ext/projects/{project_id}                   | iam:projects:update       | -            |
| GET /v3/groups                                      | iam:groups:list           | -            |
| POST /v3/groups                                     | iam:groups:create         | -            |
| GET /v3/groups/{group_id}                           | iam:groups:get            | -            |
| DELETE /v3/groups/{group_id}                        | iam:groups:delete         | -            |
| PATCH /v3/groups/{group_id}                         | iam:groups:update         | -            |
| GET /v3/groups/{group_id}/users                     | iam:groups:listUsers      | -            |
| HEAD /v3/groups/{group_id}/users/{user_id}          | iam:groups:checkUser      | -            |

| API                                                 | Action                              | Dependencies |
|-----------------------------------------------------|-------------------------------------|--------------|
| PUT /v3/groups/{group_id}/users/{user_id}           | iam:groups:addUser                  | -            |
| DELETE /v3/groups/{group_id}/users/{user_id}        | iam:groups:removeUser               | -            |
| POST /v3.0/OS-USER/users                            | iam:users:create                    | -            |
| GET /v3.0/OS-USER/users/{user_id}                   | iam:users:get                       | -            |
| PUT /v3.0/OS-USER/users/{user_id}                   | iam:users:update                    | -            |
| PUT /v3.0/OS-USER/users/{user_id}/info              | iam:users:update                    | -            |
| GET /v3/users                                       | iam:users:list                      | -            |
| POST /v3/users                                      | iam:users:create                    | -            |
| GET /v3/users/{user_id}                             | iam:users:get                       | -            |
| DELETE /v3/users/{user_id}                          | iam:users:delete                    | -            |
| PATCH /v3/users/{user_id}                           | iam:users:update                    | -            |
| GET /v3/users/{user_id}/groups                      | iam:users:listGroups                | -            |
| GET /v3.0/OS-MFA/virtual-mfa-devices                | iam:users:listVirtualMFA Devices    | -            |
| POST /v3.0/OS-MFA/virtual-mfa-devices               | iam:users:createVirtualMFADevice    | -            |
| DELETE /v3.0/OS-MFA/virtual-mfa-devices             | iam:users:deleteVirtualMFADevice    | -            |
| GET /v3.0/OS-MFA/users/{user_id}/virtual-mfa-device | iam:users:getVirtualMFA Device      | -            |
| PUT /v3.0/OS-MFA/mfa-devices/bind                   | iam:users:bindVirtualMFADevice      | -            |
| PUT /v3.0/OS-MFA/mfa-devices/unbind                 | iam:users:unbindVirtualMFADevice    | -            |
| GET /v3.0/OS-USER/login-protects                    | iam:users:listLoginProtect Settings | -            |



| API                                                         | Action                              | Dependencies |
|-------------------------------------------------------------|-------------------------------------|--------------|
| GET /v3.0/OS-USER/users/{user_id}/login-protect             | iam:users:getLoginProtectSetting    | -            |
| PUT /v3.0/OS-USER/users/{user_id}/login-protect             | iam:users:updateLoginProtectSetting | -            |
| GET /v3/OS-FEDERATION/identity_providers                    | iam:identityProviders:list          | -            |
| GET /v3/OS-FEDERATION/identity_providers/{id}               | iam:identityProviders:get           | -            |
| PUT /v3/OS-FEDERATION/identity_providers/{id}               | iam:identityProviders:create        | -            |
| DELETE /v3/OS-FEDERATION/identity_providers/{id}            | iam:identityProviders:delete        | -            |
| PATCH /v3/OS-FEDERATION/identity_providers/{id}             | iam:identityProviders:update        | -            |
| GET /v3/OS-FEDERATION/mappings                              | iam:identityProviders:listMappings  | -            |
| GET /v3/OS-FEDERATION/mappings/{id}                         | iam:identityProviders:getMapping    | -            |
| PUT /v3/OS-FEDERATION/mappings/{id}                         | iam:identityProviders:createMapping | -            |
| DELETE /v3/OS-FEDERATION/mappings/{id}                      | iam:identityProviders:deleteMapping | -            |
| PATCH /v3/OS-FEDERATION/mappings/{id}                       | iam:identityProviders:updateMapping | -            |
| GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols | iam:identityProviders:listProtocols | -            |

| API                                                                                     | Action                                   | Dependencies |
|-----------------------------------------------------------------------------------------|------------------------------------------|--------------|
| GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}               | iam:identityProviders:getProtocol        | -            |
| PUT /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}               | iam:identityProviders:createProtocol     | -            |
| DELETE /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}            | iam:identityProviders:deleteProtocol     | -            |
| PATCH /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}             | iam:identityProviders:updateProtocol     | -            |
| GET /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata  | iam:identityProviders:getSAMLMetadata    | -            |
| POST /v3-ext/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}/metadata | iam:identityProviders:createSAMLMetadata | -            |
| GET /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config               | iam:identityProviders:getOIDCConfig      | -            |
| POST /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config              | iam:identityProviders:createOIDCConfig   | -            |
| PUT /v3.0/OS-FEDERATION/identity-providers/{idp_id}/openid-connect-config               | iam:identityProviders:updateOIDCConfig   | -            |

| API                                                                | Action                                      | Dependencies |
|--------------------------------------------------------------------|---------------------------------------------|--------------|
| GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy     | iam:securityPolicies:getProtectPolicy       | -            |
| PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy     | iam:securityPolicies:updateProtectPolicy    | -            |
| GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy    | iam:securityPolicies:getPasswordPolicy      | -            |
| PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/password-policy    | iam:securityPolicies:updatePasswordPolicy   | -            |
| GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy       | iam:securityPolicies:getLoginPolicy         | -            |
| PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/login-policy       | iam:securityPolicies:updateLoginPolicy      | -            |
| GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy | iam:securityPolicies:getConsoleAclPolicy    | -            |
| PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/console-acl-policy | iam:securityPolicies:updateConsoleAclPolicy | -            |
| GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy     | iam:securityPolicies:getApiAclPolicy        | -            |
| PUT /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/api-acl-policy     | iam:securityPolicies:updateApiAclPolicy     | -            |
| GET /v3/roles                                                      | iam:roles:list                              | -            |
| GET /v3/roles/{role_id}                                            | iam:roles:get                               | -            |

| API                                                                                               | Action                         | Dependencies |
|---------------------------------------------------------------------------------------------------|--------------------------------|--------------|
| GET /v3.0/OS-PERMISSION/role-assignments                                                          | iam::listRoleAssignments       | -            |
| GET /v3/domains/{domain_id}/groups/{group_id}/roles                                               | iam:groups:listRolesOnDomain   | -            |
| GET /v3/projects/{project_id}/groups/{group_id}/roles                                             | iam:groups:listRolesOnProject  | -            |
| PUT /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}                                     | iam:groups:grantRoleOnDomain   | -            |
| PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}                                   | iam:groups:grantRoleOnProject  | -            |
| HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}                                    | iam:groups:checkRoleOnDomain   | -            |
| HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}                                  | iam:groups:checkRoleOnProject  | -            |
| GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects              | iam:groups:listRoles           | -            |
| HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects   | iam:groups:checkRole           | -            |
| DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects | iam:groups:revokeRole          | -            |
| DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}                                  | iam:groups:revokeRoleOnDomain  | -            |
| DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}                                | iam:groups:revokeRoleOnProject | -            |

| API                                                                                                            | Action                              | Dependencies |
|----------------------------------------------------------------------------------------------------------------|-------------------------------------|--------------|
| PUT /v3/OS-INHERIT/<br>domains/{domain_id}/<br>groups/{group_id}/roles/<br>{role_id}/<br>inherited_to_projects | iam:groups:grantRole                | -            |
| GET /v3.0/OS-ROLE/roles                                                                                        | iam:roles:list                      | -            |
| GET /v3.0/OS-ROLE/<br>roles/{role_id}                                                                          | iam:roles:get                       | -            |
| POST /v3.0/OS-ROLE/<br>roles                                                                                   | iam:roles:create                    | -            |
| POST /v3.0/OS-ROLE/<br>roles                                                                                   | iam:roles:create                    | -            |
| PATCH /v3.0/OS-ROLE/<br>roles/{role_id}                                                                        | iam:roles:update                    | -            |
| PATCH /v3.0/OS-ROLE/<br>roles/{role_id}                                                                        | iam:roles:update                    | -            |
| DELETE /v3.0/OS-ROLE/<br>roles/{role_id}                                                                       | iam:roles:delete                    | -            |
| GET /v3.0/OS-AGENCY/<br>agencies                                                                               | iam:agencies:list                   | -            |
| GET /v3.0/OS-AGENCY/<br>agencies/{agency_id}                                                                   | iam:agencies:get                    | -            |
| POST /v3.0/OS-AGENCY/<br>agencies                                                                              | iam:agencies:create                 | -            |
| PUT /v3.0/OS-AGENCY/<br>agencies/{agency_id}                                                                   | iam:agencies:update                 | -            |
| DELETE /v3.0/OS-<br>AGENCY/agencies/<br>{agency_id}                                                            | iam:agencies:delete                 | -            |
| GET /v3.0/OS-AGENCY/<br>domains/{domain_id}/<br>agencies/{agency_id}/<br>roles                                 | iam:agencies:listRolesOn<br>Domain  | -            |
| GET /v3.0/OS-AGENCY/<br>projects/{project_id}/<br>agencies/{agency_id}/<br>roles                               | iam:agencies:listRolesOn<br>Project | -            |

| API                                                                                                                  | Action                           | Dependencies |
|----------------------------------------------------------------------------------------------------------------------|----------------------------------|--------------|
| PUT /v3.0/OS-AGENCY/<br>domains/{domain_id}/<br>agencies/{agency_id}/<br>roles/{role_id}                             | iam:agencies:grantRoleOnDomain   | -            |
| PUT /v3.0/OS-AGENCY/<br>projects/{project_id}/<br>agencies/{agency_id}/<br>roles/{role_id}                           | iam:agencies:grantRoleOnProject  | -            |
| HEAD /v3.0/OS-AGENCY/<br>domains/{domain_id}/<br>agencies/{agency_id}/<br>roles/{role_id}                            | iam:agencies:checkRoleOnDomain   | -            |
| HEAD /v3.0/OS-AGENCY/<br>projects/{project_id}/<br>agencies/{agency_id}/<br>roles/{role_id}                          | iam:agencies:checkRoleOnProject  | -            |
| DELETE /v3.0/OS-AGENCY/<br>domains/{domain_id}/<br>agencies/{agency_id}/<br>roles/{role_id}                          | iam:agencies:revokeRoleOnDomain  | -            |
| DELETE /v3.0/OS-AGENCY/<br>projects/{project_id}/<br>agencies/{agency_id}/<br>roles/{role_id}                        | iam:agencies:revokeRoleOnProject | -            |
| GET /v3.0/OS-INHERIT/<br>domains/{domain_id}/<br>agencies/{agency_id}/<br>roles/<br>inherited_to_projects            | iam:agencies:listRoles           | -            |
| PUT /v3.0/OS-INHERIT/<br>domains/{domain_id}/<br>agencies/{agency_id}/<br>roles/{role_id}/<br>inherited_to_projects  | iam:agencies:grantRole           | -            |
| HEAD /v3.0/OS-INHERIT/<br>domains/{domain_id}/<br>agencies/{agency_id}/<br>roles/{role_id}/<br>inherited_to_projects | iam:agencies:checkRole           | -            |

| API                                                                                                      | Action                                    | Dependencies |
|----------------------------------------------------------------------------------------------------------|-------------------------------------------|--------------|
| DELETE /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects   | iam:agencies:revokeRole                   | -            |
| GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups                               | iam::listGroupsAssignedEnterpriseProject  | -            |
| GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles              | iam:groups:listRolesOnEnterpriseProject   | -            |
| PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id}    | iam:groups:grantRoleOnEnterpriseProject   | -            |
| DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/groups/{group_id}/roles/{role_id} | iam:groups:revokeRoleOnEnterpriseProject  | -            |
| GET /v3.0/OS-PERMISSION/groups/{group_id}/enterprise-projects                                            | iam:groups:listAssignedEnterpriseProjects | -            |
| GET /v3.0/OS-PERMISSION/users/{user_id}/enterprise-projects                                              | iam:users:listAssignedEnterpriseProjects  | -            |
| GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users                                | iam::listUsersAssignedEnterpriseProject   | -            |

| API                                                                                                    | Action                                     | Dependencies |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------|--------------|
| GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles              | iam:users:listRolesOnEnterpriseProject     | -            |
| PUT /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id}    | iam:users:grantRoleOnEnterpriseProject     | -            |
| DELETE /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users/{user_id}/roles/{role_id} | iam:users:revokeRoleOnEnterpriseProject    | -            |
| PUT /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments                     | iam:agencies:grantRoleOnEnterpriseProject  | -            |
| DELETE /v3.0/OS-PERMISSION/subjects/agency/scopes/enterprise-project/role-assignments                  | iam:agencies:revokeRoleOnEnterpriseProject | -            |
| GET /v5/asymmetric-signature-switch                                                                    | iam::getAsymmetricSignatureSwitchV5        | -            |
| PUT /v5/asymmetric-signature-switch                                                                    | iam::setAsymmetricSignatureSwitchV5        | -            |
| GET /v5/mfa-devices                                                                                    | iam:mfa:listMFADevicesV5                   | -            |
| POST /v5/virtual-mfa-devices                                                                           | iam:mfa:createVirtualMFADeviceV5           | -            |
| DELETE /v5/virtual-mfa-devices                                                                         | iam:mfa:deleteVirtualMFADeviceV5           | -            |
| POST /v5/mfa-devices/enable                                                                            | iam:mfa:enableV5                           | -            |
| POST /v5/mfa-devices/disable                                                                           | iam:mfa:disableV5                          | -            |



| API                                                           | Action                                      | Dependencies |
|---------------------------------------------------------------|---------------------------------------------|--------------|
| GET /v5/password-policy                                       | iam:securitypolicies:getPasswordPolicyV5    | -            |
| PUT /v5/password-policy                                       | iam:securitypolicies:updatePasswordPolicyV5 | -            |
| GET /v5/login-policy                                          | iam:securitypolicies:getLoginPolicyV5       | -            |
| PUT /v5/login-policy                                          | iam:securitypolicies:updateLoginPolicyV5    | -            |
| GET /v5/users/{user_id}/access-keys                           | iam:credentials:listCredentialsV5           | -            |
| GET /v5/users/{user_id}/access-keys/{access_key_id}/last-used | iam:credentials:showAccessKeyLastUsedV5     | -            |
| POST /v5/users/{user_id}/access-keys                          | iam:credentials:createCredentialV5          | -            |
| PUT /v5/users/{user_id}/access-keys/{access_key_id}           | iam:credentials:updateCredentialV5          | -            |
| DELETE /v5/users/{user_id}/access-keys/{access_key_id}        | iam:credentials:deleteCredentialV5          | -            |
| POST /v5/caller-password                                      | iam:users:changePasswordV5                  | -            |
| GET /v5/users/{user_id}/login-profile                         | iam:users:showLoginProfileV5                | -            |
| POST /v5/users/{user_id}/login-profile                        | iam:users:createLoginProfileV5              | -            |
| PUT /v5/users/{user_id}/login-profile                         | iam:users:updateLoginProfileV5              | -            |
| DELETE /v5/users/{user_id}/login-profile                      | iam:users:deleteLoginProfileV5              | -            |
| GET /v5/users                                                 | iam:users:listUsersV5                       | -            |
| GET /v5/users/{user_id}                                       | iam:users:getUserV5                         | -            |
| GET /v5/users/{user_id}/last-login                            | iam:users:showUserLastLoginV5               | -            |
| POST /v5/users                                                | iam:users:createUserV5                      | -            |
| PUT /v5/users/{user_id}                                       | iam:users:updateUserV5                      | -            |

| API                                                             | Action                                | Dependencies |
|-----------------------------------------------------------------|---------------------------------------|--------------|
| DELETE /v5/users/{user_id}                                      | iam:users:deleteUserV5                | -            |
| GET /v5/groups                                                  | iam:groups:listGroupsV5               | -            |
| GET /v5/groups/{group_id}                                       | iam:groups:getGroupV5                 | -            |
| POST /v5/groups                                                 | iam:groups:createGroupV5              | -            |
| PUT /v5/groups/{group_id}                                       | iam:groups:updateGroupV5              | -            |
| DELETE /v5/groups/{group_id}                                    | iam:groups:deleteGroupV5              | -            |
| POST /v5/groups/{group_id}/add-user                             | iam:permissions:addUserToGroupV5      | -            |
| POST /v5/groups/{group_id}/remove-user                          | iam:permissions:removeUserFromGroupV5 | -            |
| GET /v5/policies                                                | iam:policies:listV5                   | -            |
| GET /v5/policies/{policy_id}                                    | iam:policies:getV5                    | -            |
| POST /v5/policies                                               | iam:policies:createV5                 | -            |
| DELETE /v5/policies/{policy_id}                                 | iam:policies:deleteV5                 | -            |
| GET /v5/policies/{policy_id}/versions                           | iam:policies:listVersionsV5           | -            |
| GET /v5/policies/{policy_id}/versions/{version_id}              | iam:policies:getVersionV5             | -            |
| POST /v5/policies/{policy_id}/versions                          | iam:policies:createVersionV5          | -            |
| DELETE /v5/policies/{policy_id}/versions/{version_id}           | iam:policies:deleteVersionV5          | -            |
| POST /v5/policies/{policy_id}/versions/{version_id}/set-default | iam:policies:setDefaultVersionV5      | -            |
| POST /v5/policies/{policy_id}/attach-agency                     | iam:agencies:attachPolicyV5           | -            |
| POST /v5/policies/{policy_id}/attach-group                      | iam:groups:attachPolicyV5             | -            |

| API                                                              | Action                                              | Dependencies |
|------------------------------------------------------------------|-----------------------------------------------------|--------------|
| POST /v5/policies/{policy_id}/attach-user                        | iam:users:attachPolicyV5                            | -            |
| POST /v5/policies/{policy_id}/detach-agency                      | iam:agencies:detachPolicyV5                         | -            |
| POST /v5/policies/{policy_id}/detach-group                       | iam:groups:detachPolicyV5                           | -            |
| POST /v5/policies/{policy_id}/detach-user                        | iam:users:detachPolicyV5                            | -            |
| GET /v5/policies/{policy_id}/attached-entities                   | iam:policies:listEntitiesV5                         | -            |
| GET /v5/agencies/{agency_id}/attached-policies                   | iam:agencies:listAttachedPoliciesV5                 | -            |
| GET /v5/groups/{group_id}/attached-policies                      | iam:groups:listAttachedPoliciesV5                   | -            |
| GET /v5/users/{user_id}/attached-policies                        | iam:users:listAttachedPoliciesV5                    | -            |
| PUT /v5/service-linked-agencies                                  | iam:agencies:createServiceLinkedAgencyV5            | -            |
| DELETE /v5/service-linked-agencies/{agency_id}                   | iam:agencies:deleteServiceLinkedAgencyV5            | -            |
| GET /v5/service-linked-agencies/deletion-task/{deletion_task_id} | iam:agencies:getServiceLinkedAgencyDeletionStatusV5 | -            |
| GET /v5/agencies                                                 | iam:agencies:listV5                                 | -            |
| GET /v5/agencies/{agency_id}                                     | iam:agencies:getV5                                  | -            |
| POST /v5/agencies                                                | iam:agencies:createV5                               | -            |
| PUT /v5/agencies/{agency_id}                                     | iam:agencies:updateV5                               | -            |
| DELETE /v5/agencies/{agency_id}                                  | iam:agencies:deleteV5                               | -            |
| PUT /v5/agencies/{agency_id}/trust-policy                        | iam:agencies:updateTrustPolicyV5                    | -            |

| API                                                  | Action                     | Dependencies |
|------------------------------------------------------|----------------------------|--------------|
| GET /v5/{resource_type}/{resource_id}/tags           | iam::listTagsForResourceV5 | -            |
| POST /v5/{resource_type}/{resource_id}/tags/create   | iam::tagForResourceV5      | -            |
| DELETE /v5/{resource_type}/{resource_id}/tags/delete | iam::untagForResourceV5    | -            |
| GET /v5/account-summary                              | iam::getAccountSummaryV5   | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-241](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for IAM.

**Table 3-241** Resource types supported by IAM

| Resource Type | URN                                              |
|---------------|--------------------------------------------------|
| agency        | iam::<account-id>:agency:<agency-name-with-path> |
| policy        | iam::<account-id>:policy:<policy-name-with-path> |
| user          | iam::<account-id>:user:<user-name>               |
| mfa           | iam::<account-id>:mfa:<mfa-name>                 |
| group         | iam::<account-id>:group:<group-name>             |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.

- Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, iam) apply only to operations of the xx service. For details, see [Table 3-242](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

#### Service-specific condition keys supported by IAM

The following table lists the condition keys that you can define in identity policies for IAM. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-242** Service-specific condition keys supported by IAM

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                                 |
|--------------------------------|--------|-------------------------------|-------------------------------------------------------------------------------------------------------------|
| iam:PolicyURN                  | string | Single-valued                 | Filters access by the URN of an identity policy.                                                            |
| iam:ServicePrincipal           | string | Single-valued                 | Filters access by the service principal of the cloud service to which this service linked agency is passed. |

## 3.14.2 Organizations

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by Organizations, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Organizations, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Organizations.

**Table 3-243** Actions supported by Organizations

| Action                                     | Description                                                   | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|--------------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| organizations:<br>organizations:<br>create | Grants permission to create an organization.                  | Write        | -                           | -                                                                                                                                 | -     |
| organizations:<br>organizations:<br>get    | Grants permission to show information about the organization. | Read         | -                           | -                                                                                                                                 | -     |
| organizations:<br>organizations:<br>delete | Grants permission to delete the organization.                 | Write        | -                           | -                                                                                                                                 | -     |
| organizations:<br>organizations:<br>leave  | Grants permission to leave the current organization.          | Write        | -                           | -                                                                                                                                 | -     |
| organizations:<br>roots:list               | Grants permission to list roots of the organization.          | List         | -                           | -                                                                                                                                 | -     |
| organizations:<br>ous:create               | Grants permission to create an organizational unit.           | Write        | ou                          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                            |                                                               |              | root                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                                            |                                                               |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| organizations:<br>ous:list                 | Grants permission to list organizational units.               | List         | -                           | -                                                                                                                                 | -     |

| Action                        | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|-------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| organizations:ous:get         | Grants permission to show information about the organizational unit. | Read         | ou *                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations:ous:update      | Grants permission to update the name of the organizational unit.     | Write        | ou *                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations:ous:delete      | Grants permission to delete the organizational unit.                 | Write        | ou *                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations:accounts:create | Grants permission to create an account.                              | Write        | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | -     |
| organizations:accounts:list   | Grants permission to list accounts.                                  | List         | -                           | -                                                                                                                                 | -     |
| organizations:accounts:get    | Grants permission to show information about an account.              | Read         | account *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations:accounts:remove | Grants permission to remove the specified account.                   | Write        | account *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations:accounts:move   | Grants permission to move an account.                                | Write        | account *                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |



| Action                                   | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| organizations:accounts:invite            | Grants permission to invite an account to the organization.            | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | -     |
| organizations:createAccountStatuses:list | Grants permission to list create account statuses.                     | List         | -                           | -                                                                                                                                     | -     |
| organizations:createAccountStatuses:get  | Grants permission to show information about the create account status. | Read         | -                           | -                                                                                                                                     | -     |
| organizations:handshakes:get             | Grants permission to show information about the handshake.             | Read         | handshake*                  | -                                                                                                                                     | -     |
| organizations:handshakes:accept          | Grants permission to accept the handshake.                             | Write        | handshake*                  | -                                                                                                                                     | -     |
| organizations:handshakes:decline         | Grants permission to decline the handshake.                            | Write        | handshake*                  | -                                                                                                                                     | -     |
| organizations:handshakes:cancel          | Grants permission to cancel the handshake.                             | Write        | handshake*                  | -                                                                                                                                     | -     |
| organizations:receivedHandshakes:list    | Grants permission to list received handshakes.                         | List         | -                           | -                                                                                                                                     | -     |

| Action                                           | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key                   | Alias |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------|-------|
| organizations:handshakes:list                    | Grants permission to list handshakes.                                                            | List         | -                           | -                               | -     |
| organizations:trustedServices:enable             | Grants permission to enable a trusted service.                                                   | Write        | -                           | organization s:ServicePrincipal | -     |
| organizations:trustedServices:disable            | Grants permission to disable a trusted service.                                                  | Write        | -                           | organization s:ServicePrincipal | -     |
| organizations:trustedServices:list               | Grants permission to list trusted services for the organization.                                 | List         | -                           | -                               | -     |
| organizations:delegatedAdministrators:register   | Grants permission to register a delegated administrator for a service.                           | Write        | account *                   | g:ResourceTag/<tag-key>         | -     |
|                                                  |                                                                                                  |              | -                           | organization s:ServicePrincipal |       |
| organizations:delegatedAdministrators:deregister | Grants permission to deregister a delegated administrator of a service.                          | Write        | account *                   | g:ResourceTag/<tag-key>         | -     |
|                                                  |                                                                                                  |              | -                           | organization s:ServicePrincipal |       |
| organizations:delegatedServices:list             | Grants permission to list services for which the specified account is a delegated administrator. | List         | account *                   | g:ResourceTag/<tag-key>         | -     |

| Action                                       | Description                                                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| organizations: delegatedAdministrators: list | Grants permission to list the accounts that are designated as delegated administrators in this organization. | List         | -                           | <a href="#">organization:ServicePrincipal</a>                                                                                     | -     |
| organizations: policies:create               | Grants permission to create a policy.                                                                        | Write        | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | -     |
| organizations: policies:list                 | Grants permission to list policies.                                                                          | List         | -                           | -                                                                                                                                 | -     |
| organizations: policies:get                  | Grants permission to show information about the policy.                                                      | Read         | policy *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations: policies:update               | Grants permission to update the policy.                                                                      | Write        | policy *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations: policies:delete               | Grants permission to delete the policy.                                                                      | Write        | policy *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| organizations: policies:enable               | Grants permission to enable a policy type in a root.                                                         | Write        | root *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |

| Action                              | Description                                                                          | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|-------------------------------------|--------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| organizations:policies:disable      | Grants permission to disable a policy type in a root.                                | Write        | root *                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| organizations:policies:attach       | Grants permission to attach a policy to an entity.                                   | Write        | policy *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                     |                                                                                      |              | account                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
|                                     |                                                                                      |              | ou                          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
|                                     |                                                                                      |              | root                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| organizations:policies:detach       | Grants permission to detach a policy from an entity.                                 | Write        | policy *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                     |                                                                                      |              | account                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
|                                     |                                                                                      |              | ou                          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
|                                     |                                                                                      |              | root                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| organizations:attachedEntities:list | Grants permission to list all the entities that the specified policy is attached to. | List         | policy *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| organizations:tags:list             | Grants permission to list tags that are attached to the specified resource.          | List         | account                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                     |                                                                                      |              | ou                          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
|                                     |                                                                                      |              | root                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
|                                     |                                                                                      |              | policy                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |

| Action                        | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|-------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| organizations:resources:tag   | Grants permission to add tags to the specified resource.                                  | Tagging      | account                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                               |                                                                                           |              | ou                          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                               |                                                                                           |              | root                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                               |                                                                                           |              | policy                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                               |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| organizations:resources:untag | Grants permission to remove any tags with the specified keys from the specified resource. | Tagging      | account                     | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                               |                                                                                           |              | ou                          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                               |                                                                                           |              | root                        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                               |                                                                                           |              | policy                      | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                               |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| organizations:entities:list   | Grants permission to list roots, organizational units and accounts in the organization.   | List         | -                           | -                                                                                                                                 | -     |

| Action                               | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| organizations:services:list          | Grants permission to list all services that could integrate with Organizations Service.         | List         | -                           | -             | -     |
| organizations:tagPolicyServices:list | Grants permission to lists resource types added to tag policy enforcement.                      | List         | -                           | -             | -     |
| organizations:effectivePolicies:get  | Grants permission to show effective policies for specified policy type and account.             | Read         | -                           | -             | -     |
| organizations:resources:listByTag    | Grants permission to list all resource types and tag information query instances.               | List         | -                           | -             | -     |
| organizations:resources:countByTag   | Grants permission to list resource types and tag information and query the number of instances. | List         | -                           | -             | -     |
| organizations:resources:list         | Grants permission to list item labels.                                                          | List         | -                           | -             | -     |

| Action                    | Description                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------|---------------------------------------------------|--------------|-----------------------------|---------------|-------|
| organizations:quotas:list | Grants permission to list quotas of organization. | List         | -                           | -             | -     |

Each API of Organizations usually supports one or more actions. [Table 3-244](#) lists the supported actions and dependencies.

**Table 3-244** Actions and dependencies supported by Organizations APIs

| API                                                                 | Action                             | Dependencies                             |
|---------------------------------------------------------------------|------------------------------------|------------------------------------------|
| POST /v1/organizations                                              | organizations:organizations:create | iam:agencies:createServiceLinkedAgencyV5 |
| GET /v1/organizations                                               | organizations:organizations:get    | -                                        |
| DELETE /v1/organizations                                            | organizations:organizations:delete | -                                        |
| POST /v1/organizations/leave                                        | organizations:organizations:leave  | -                                        |
| GET /v1/organizations/roots                                         | organizations:roots:list           | -                                        |
| POST /v1/organizations/organizational-units                         | organizations:ous:create           | organizations:resources:tag              |
| GET /v1/organizations/organizational-units                          | organizations:ous:list             | -                                        |
| GET /v1/organizations/organizational-units/{organizational_unit_id} | organizations:ous:get              | -                                        |

| API                                                                                        | Action                                       | Dependencies                |
|--------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------|
| PATCH /v1/<br>organizations/<br>organizational-<br>units/<br>{organizational_unit<br>_id}  | organizations:ous:update                     | -                           |
| DELETE /v1/<br>organizations/<br>organizational-<br>units/<br>{organizational_unit<br>_id} | organizations:ous:delete                     | -                           |
| POST /v1/<br>organizations/<br>accounts                                                    | organizations:accounts:crea<br>te            | organizations:resources:tag |
| GET /v1/<br>organizations/<br>accounts                                                     | organizations:accounts:list                  | -                           |
| GET /v1/<br>organizations/<br>accounts/<br>{account_id}                                    | organizations:accounts:get                   | -                           |
| POST /v1/<br>organizations/<br>accounts/<br>{account_id}/<br>remove                        | organizations:accounts:rem<br>ove            | -                           |
| POST /v1/<br>organizations/<br>accounts/<br>{account_id}/move                              | organizations:accounts:mov<br>e              | -                           |
| PATCH /v1/<br>organizations/<br>accounts/<br>{account_id}                                  | organizations:accounts:upd<br>ate            | -                           |
| POST /v1/<br>organizations/<br>accounts/invite                                             | organizations:accounts:invit<br>e            | organizations:resources:tag |
| GET /v1/<br>organizations/<br>create-account-<br>status                                    | organizations:createAccoun<br>tStatuses:list | -                           |



| API                                                                    | Action                                  | Dependencies                             |
|------------------------------------------------------------------------|-----------------------------------------|------------------------------------------|
| POST /v1/organizations/accounts/{account_id}/close                     | organizations:accounts:close            | -                                        |
| GET /v1/organizations/close-account-status                             | organizations:closeAccountStatuses:list | -                                        |
| GET /v1/organizations/create-account-status/{create_account_status_id} | organizations:createAccountStatuses:get | -                                        |
| GET /v1/organizations/handshakes/{handshake_id}                        | organizations:handshakes:get            | -                                        |
| POST /v1/received-handshakes/{handshake_id}/accept                     | organizations:handshakes:accept         | iam:agencies:createServiceLinkedAgencyV5 |
| POST /v1/received-handshakes/{handshake_id}/decline                    | organizations:handshakes:decline        | -                                        |
| POST /v1/organizations/handshakes/{handshake_id}/cancel                | organizations:handshakes:cancel         | -                                        |
| GET /v1/received-handshakes                                            | organizations:receivedHandshakes:list   | -                                        |
| GET /v1/organizations/handshakes                                       | organizations:handshakes:list           | -                                        |
| POST /v1/organizations/trusted-services/enable                         | organizations:trustedServices:enable    | -                                        |
| POST /v1/organizations/trusted-services/disable                        | organizations:trustedServices:disable   | -                                        |

| API                                                            | Action                                           | Dependencies                |
|----------------------------------------------------------------|--------------------------------------------------|-----------------------------|
| GET /v1/organizations/trusted-services                         | organizations:trustedServices:list               | -                           |
| POST /v1/organizations/delegated-administrators/register       | organizations:delegatedAdministrators:register   | -                           |
| POST /v1/organizations/delegated-administrators/deregister     | organizations:delegatedAdministrators:deregister | -                           |
| GET /v1/organizations/accounts/{account_id}/delegated-services | organizations:delegatedServices:list             | -                           |
| GET /v1/organizations/delegated-administrators                 | organizations:delegatedAdministrators:list       | -                           |
| POST /v1/organizations/policies                                | organizations:policies:create                    | organizations:resources:tag |
| GET /v1/organizations/policies                                 | organizations:policies:list                      | -                           |
| GET /v1/organizations/policies/{policy_id}                     | organizations:policies:get                       | -                           |
| PATCH /v1/organizations/policies/{policy_id}                   | organizations:policies:update                    | -                           |
| DELETE /v1/organizations/policies/{policy_id}                  | organizations:policies:delete                    | -                           |
| POST /v1/organizations/policies/enable                         | organizations:policies:enable                    | -                           |
| POST /v1/organizations/policies/disable                        | organizations:policies:disable                   | -                           |

| API                                                          | Action                               | Dependencies |
|--------------------------------------------------------------|--------------------------------------|--------------|
| POST /v1/organizations/policies/{policy_id}/attach           | organizations:policies:attach        | -            |
| POST /v1/organizations/policies/{policy_id}/detach           | organizations:policies:detach        | -            |
| GET /v1/organizations/policies/{policy_id}/attached-entities | organizations:attachedEntities:list  | -            |
| GET /v1/organizations/resources/{resource_id}/tags           | organizations:tags:list              | -            |
| POST /v1/organizations/resources/{resource_id}/tag           | organizations:resources:tag          | -            |
| POST /v1/organizations/resources/{resource_id}/untag         | organizations:resources:untag        | -            |
| GET /v1/organizations/entities                               | organizations:entities:list          | -            |
| GET /v1/organizations/services                               | organizations:services:list          | -            |
| GET /v1/organizations/tag-policy-services                    | organizations:tagPolicyServices:list | -            |
| GET /v1/organizations/entities/effective-policies            | organizations:effectivePolicies:get  | -            |
| GET /v1/organizations/{resource_type}/{resource_id}/tags     | organizations:tags:list              | -            |

| API                                                              | Action                             | Dependencies |
|------------------------------------------------------------------|------------------------------------|--------------|
| POST /v1/organizations/{resource_type}/{resource_id}/tags/create | organizations:resources:tag        | -            |
| POST /v1/organizations/{resource_type}/{resource_id}/tags/delete | organizations:resources:untag      | -            |
| POST /v1/organizations/{resource_type}/resource-instances/filter | organizations:resources:listByTag  | -            |
| POST /v1/organizations/{resource_type}/resource-instances/count  | organizations:resources:countByTag | -            |
| GET /v1/organizations/{resource_type}/tags                       | organizations:resources:list       | -            |
| GET /v1/organizations/quotas                                     | organizations:quotas:list          | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-245](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for Organizations.

**Table 3-245** Resource types supported by Organizations

| Resource Type | URN                                                    |
|---------------|--------------------------------------------------------|
| builtinpolicy | organizations::system:policy:<policy-type>/<policy-id> |

| Resource Type | URN                                                                                       |
|---------------|-------------------------------------------------------------------------------------------|
| ou            | organizations::<management-account-id>:ou:<organization-id>/<organization-unit-id>        |
| root          | organizations::<management-account-id>:root:<organization-id>/<root-id>                   |
| organization  | organizations::<management-account-id>:organization:<organization-id>                     |
| account       | organizations::<management-account-id>:account:<organization-id>/<account-id>             |
| policy        | organizations::<management-account-id>:policy:<organization-id>/<policy-type>/<policy-id> |
| handshake     | organizations::<management-account-id>:handshake:<organization-id>/<handshake-id>         |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, organizations) apply only to operations of the xx service. For details, see [Table 3-246](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by Organizations

The following table lists the condition keys that you can define in identity policies for Organizations. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-246** Service-specific condition keys supported by Organizations

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                          |
|--------------------------------|--------|-------------------------------|----------------------------------------------------------------------|
| organizations:ServicePrincipal | string | Single-valued                 | Filters access based on the specified name of the service principal. |

### 3.14.3 Resource Access Manager (RAM)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.

- You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
- If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
- Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by RAM, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by RAM, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for RAM.

**Table 3-247** Actions supported by RAM

| Action               | Description                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ram:permissions:list | Grants permission to list the RAM permissions.              | List         | permission *                | -             | -     |
| ram:permissions:get  | Grants permission to get the contents of an RAM permission. | Read         | permission *                | -             | -     |

| Action                    | Description                                                                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                | Alias |
|---------------------------|----------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| ram:resourceShares:create | Grants permission to create a resource share with provided resource(s) and/or principal(s).        | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">ram:RequestedResourceType</a></li> <li>• <a href="#">ram:ResourceUrn</a></li> <li>• <a href="#">ram:Principal</a></li> <li>• <a href="#">ram:TargetOrgPaths</a></li> <li>• <a href="#">ram:RequestedAllowExternalPrincipals</a></li> </ul> | -     |
| ram:resourceShares:search | Grants permission to get a set of resource shares from a provided list or with a specified status. | Read         | -                           | <a href="#">g:TagKeys</a>                                                                                                                                                                                                                                                                                                                                                                    | -     |
| ram:resourceShares:update | Grants permission to update attributes of the resource share.                                      | Write        | resourceShare *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">ram:AllowExternalPrincipals</a></li> </ul>                                                                                                                                                                                                                                     | -     |
|                           |                                                                                                    |              | -                           | <a href="#">ram:RequestedAllowExternalPrincipals</a>                                                                                                                                                                                                                                                                                                                                         |       |



| Action                          | Description                                                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                   | Alias |
|---------------------------------|------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| ram:resourceShares:delete       | Grants permission to delete resource share.                                              | Write        | resourceShare *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">ram:AllowExternalPrincipals</a></li> </ul>                                                                        | -     |
| ram:resourceShares:associate    | Grants permission to associate resource(s) and/or principal(s) to a resource share.      | Write        | resourceShare *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">ram:AllowExternalPrincipals</a></li> </ul>                                                                        | -     |
|                                 |                                                                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">ram:RequestedResourceType</a></li> <li>• <a href="#">ram:ResourceUrn</a></li> <li>• <a href="#">ram:Principal</a></li> <li>• <a href="#">ram:TargetOrgPaths</a></li> </ul> |       |
| ram:resourceShares:disassociate | Grants permission to disassociate resource(s) and/or principal(s) from a resource share. | Write        | resourceShare *             | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">ram:AllowExternalPrincipals</a></li> </ul>                                                                        | -     |
|                                 |                                                                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">ram:RequestedResourceType</a></li> <li>• <a href="#">ram:ResourceUrn</a></li> <li>• <a href="#">ram:Principal</a></li> <li>• <a href="#">ram:TargetOrgPaths</a></li> </ul> |       |

| Action                                             | Description                                                                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| ram:resourceShares:searchResourceShareAssociations | Grants permission to get a set of resource share associations from a provided list or with a specified status of the specified type. | Read         | -                           | -                                                                                                                                 | -     |
| ram:resourceShares:associatePermission             | Grants permission to associate a permission with a resource share.                                                                   | Write        | resourceShare *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                                    |                                                                                                                                      |              | -                           | <a href="#">ram:PermissionUrn</a>                                                                                                 |       |
| ram:resourceShares:disassociatePermission          | Grants permission to disassociate a permission from a resource share.                                                                | Write        | resourceShare *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                                    |                                                                                                                                      |              | -                           | <a href="#">ram:PermissionUrn</a>                                                                                                 |       |
| ram:resourceShares:listAssociatedPermissions       | Grants permission to list the permissions associated with a resource share.                                                          | List         | resourceShare *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| ram:resourceShares:tag                             | Grants permission to tag the specified resource share.                                                                               | Tagging      | resourceShare *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                                    |                                                                                                                                      |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |

| Action                                           | Description                                                                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| ram:resourceShares:untag                         | Grants permission to untag the specified resource share.                                                             | Tagging      | resourceShare *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -     |
|                                                  |                                                                                                                      |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| ram:resourceShares:listTags                      | Grants permission to query resource share tags.                                                                      | List         | -                           | -                                                                                                                                     | -     |
| ram:resourceShares:listResourceSharesByTag       | Grants permission to query the resource shares based on the tag.                                                     | List         | -                           | <a href="#">g:TagKeys</a>                                                                                                             | -     |
| ram:resourceShares:searchResourceShareCountByTag | Grants permission to query the number of resource shares based on the tag.                                           | Read         | -                           | <a href="#">g:TagKeys</a>                                                                                                             | -     |
| ram:sharedResources:search                       | Grants permission to list the resources that you added to resource shares or the resources that are shared with you. | List         | -                           | -                                                                                                                                     | -     |

| Action                              | Description                                                                                                          | Access Level | Resource Type (*: required) | Condition Key           | Alias |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------|-------|
| ram:sharedPrincipals:search         | Grants permission to list the principals that you have shared resources with or that have shared resources with you. | List         | -                           | -                       | -     |
| ram:resourceShareInvitations:accept | Grants permission to accept the specified resource share invitation.                                                 | Write        | resourceShareInvitation *   | -                       | -     |
|                                     |                                                                                                                      |              | -                           | ram:ShareOwnerAccountId |       |
| ram:resourceShareInvitations:reject | Grants permission to reject the specified resource share invitation.                                                 | Write        | resourceShareInvitation *   | -                       | -     |
|                                     |                                                                                                                      |              | -                           | ram:ShareOwnerAccountId |       |
| ram:resourceShareInvitations:search | Grants permission to get resource share invitations by the specified invitation id or resource share id.             | Read         | -                           | -                       | -     |

| Action                                                 | Description                                                                                                                            | Access Level          | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------------|---------------|-------|
| ram:resourceShares:enableSharingWithOrganization       | Grants permission to enable resource sharing with Organizations.                                                                       | Permission_management | -                           | -             | -     |
| ram:resourceShares:disableSharingWithOrganization      | Grants permission to disable resource sharing with Organizations.                                                                      | Permission_management | -                           | -             | -     |
| ram:resourceShares:searchEnableSharingWithOrganization | Grants permission to check whether resource sharing with Organizations is enabled.                                                     | Read                  | -                           | -             | -     |
| ram:sharedResources:searchDistinctResource             | Grants permission to list the distinct resources that you added to resource shares or the distinct resources that are shared with you. | List                  | -                           | -             | -     |

| Action                                       | Description                                                                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ram:sharedPrincipals:searchDistinctPrincipal | Grants permission to list the distinct principals that you have shared resources with or that have shared resources with you. | List         | -                           | -             | -     |
| ram:resourceShares:listQuota                 | Grants permission to list quotas.                                                                                             | List         | -                           | -             | -     |
| ram:resourceTypes:list                       | Grants permission to list resource type.                                                                                      | List         | -                           | -             | -     |
| ram:permission:listVersions                  | Grants permission to list all of the versions of specified RAM permission.                                                    | List         | -                           | -             | -     |

Each API of RAM usually supports one or more actions. [Table 3-248](#) lists the supported actions and dependencies.

**Table 3-248** Actions and dependencies supported by RAM APIs

| API                                 | Action                    | Dependencies |
|-------------------------------------|---------------------------|--------------|
| GET /v1/permissions                 | ram:permissions:list      | -            |
| GET /v1/permissions/{permission_id} | ram:permissions:get       | -            |
| POST /v1/resource-shares            | ram:resourceShares:create | -            |

| API                                                                  | Action                                             | Dependencies |
|----------------------------------------------------------------------|----------------------------------------------------|--------------|
| POST /v1/resource-shares/search                                      | ram:resourceShares:search                          | -            |
| PUT /v1/resource-shares/{resource_share_id}                          | ram:resourceShares:update                          | -            |
| DELETE /v1/resource-shares/{resource_share_id}                       | ram:resourceShares:delete                          | -            |
| POST /v1/resource-shares/{resource_share_id}/associate               | ram:resourceShares:associate                       | -            |
| POST /v1/resource-shares/{resource_share_id}/disassociate            | ram:resourceShares:disassociate                    | -            |
| POST /v1/resource-share-associations/search                          | ram:resourceShares:searchResourceShareAssociations | -            |
| POST /v1/resource-shares/{resource_share_id}/associate-permission    | ram:resourceShares:associatePermission             | -            |
| POST /v1/resource-shares/{resource_share_id}/disassociate-permission | ram:resourceShares:disassociatePermission          | -            |
| GET /v1/resource-shares/{resource_share_id}/associated-permissions   | ram:resourceShares:listAssociatedPermissions       | -            |
| POST /v1/resource-shares/{resource_share_id}/tags/create             | ram:resourceShares:tag                             | -            |
| POST /v1/resource-shares/{resource_share_id}/tags/delete             | ram:resourceShares:untag                           | -            |

| API                                                                       | Action                                                 | Dependencies |
|---------------------------------------------------------------------------|--------------------------------------------------------|--------------|
| GET /v1/resource-shares/tags                                              | ram:resourceShares:listTags                            | -            |
| POST /v1/resource-shares/resource-instances/filter                        | ram:resourceShares:listResourceSharesByTag             | -            |
| POST /v1/resource-shares/resource-instances/count                         | ram:resourceShares:searchResourceShareCountByTag       | -            |
| POST /v1/shared-resources/search                                          | ram:sharedResources:search                             | -            |
| POST /v1/shared-principals/search                                         | ram:sharedPrincipals:search                            | -            |
| POST /v1/resource-share-invitations/{resource_share_invitation_id}/accept | ram:resourceShareInvitations:accept                    | -            |
| POST /v1/resource-share-invitations/{resource_share_invitation_id}/reject | ram:resourceShareInvitations:reject                    | -            |
| POST /v1/resource-share-invitations/search                                | ram:resourceShareInvitations:search                    | -            |
| POST /v1/organization-share/enable                                        | ram:resourceShares:enableSharingWithOrganization       | -            |
| POST /v1/organization-share/disable                                       | ram:resourceShares:disableSharingWithOrganization      | -            |
| GET /v1/organization-share                                                | ram:resourceShares:searchEnableSharingWithOrganization | -            |
| POST /v1/shared-resources/search-distinct-resource                        | ram:sharedResources:searchDistinctResource             | -            |
| POST /v1/shared-principals/search-distinct-principal                      | ram:sharedPrincipals:searchDistinctPrincipal           | -            |
| GET /v1/resource-shares/quotas                                            | ram:resourceShares:listQuota                           | -            |



| API                                          | Action                       | Dependencies |
|----------------------------------------------|------------------------------|--------------|
| GET /v1/resource-types                       | ram:resourceTypes:list       | -            |
| GET /v1/permissions/{permission_id}/versions | ram:permissions:listVersions | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-249](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for RAM.

**Table 3-249** Resource types supported by RAM

| Resource Type           | URN                                                                      |
|-------------------------|--------------------------------------------------------------------------|
| resourceShare           | ram::<account-id>:resourceShare:<resource-share-id>                      |
| resourceShareInvitation | ram::<account-id>:resourceShareInvitation:<resource-share-invitation-id> |
| permission              | ram::system:permission:<permission-id>                                   |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, ram) apply only to operations of the xx service. For details, see [Table 3-250](#).

- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by RAM

The following table lists the condition keys that you can define in identity policies for RAM. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-250** Service-specific condition keys supported by RAM

| Service-specific Condition Key         | Type   | Single-valued/<br>Multivalued | Description                                                            |
|----------------------------------------|--------|-------------------------------|------------------------------------------------------------------------|
| <code>ram:RequestedResourceType</code> | string | Multivalued                   | Filters access based on the specified resource type.                   |
| <code>ram:ResourceUrn</code>           | string | Multivalued                   | Filters access based on a resource with the specified URN.             |
| <code>ram:Principal</code>             | string | Multivalued                   | Filters access based on the format of the specified principal.         |
| <code>ram:TargetOrgPaths</code>        | string | Multivalued                   | Filters access based on the specified organization path of principals. |
| <code>ram:PermissionUrn</code>         | string | Single-valued                 | Filters access based on the specified Permission URN.                  |

| Service-specific Condition Key       | Type    | Single-valued/<br>Multivalued | Description                                                                                                                                                                                                                                                                                 |
|--------------------------------------|---------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ram:ShareOwnerAccountId              | string  | Single-valued                 | Filters access based on resource shares owned by a specific account. For example, you can use this condition key to specify which resource share invitations can be accepted or rejected based on the resource share owner's account ID.                                                    |
| ram:AllowExternalPrincipals          | boolean | Single-valued                 | Filters access by resource shares that allow or deny sharing with external principals. For example, specify true if the action can only be performed on resource shares that allow sharing with external principals. External principals are accounts that are outside of its Organization. |
| ram:RequestedAllowExternalPrincipals | boolean | Single-valued                 | Filters access by the specified value for 'allow_external_principals'. External principals are accounts that are outside of its Organization.                                                                                                                                               |

### 3.14.4 IAM Identity Center

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational

unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by IdentityCenter, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by IdentityCenter, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for IdentityCenter.

**Table 3-251** Actions supported by IdentityCenter

| Action                             | Description                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------|-------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:user:create         | Grants permission to create a user.             | Write        | -                           | -             | -     |
| IdentityCenter:user:list           | Grants permission to query the user list.       | Read         | -                           | -             | -     |
| IdentityCenter:user:describe       | Grants permission to query user details.        | Read         | -                           | -             | -     |
| IdentityCenter:user:describe Users | Grants permission to batch obtain user details. | Read         | -                           | -             | -     |
| IdentityCenter:user:update         | Grants permission to update a user.             | Write        | -                           | -             | -     |
| IdentityCenter:user:delete         | Grants permission to delete a user.             | Write        | -                           | -             | -     |
| IdentityCenter:user:getUserId      | Grants permission to obtain the user ID.        | Read         | -                           | -             | -     |
| IdentityCenter:user:enableUser     | Grants permission to enable a user.             | Write        | -                           | -             | -     |
| IdentityCenter:user:disableUser    | Grants permission to disable a user.            | Write        | -                           | -             | -     |
| IdentityCenter:group:create        | Grants permission to create a group.            | Write        | -                           | -             | -     |

| Action                                       | Description                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:group:list                    | Grants permission to query the group list.                     | Read         | -                           | -             | -     |
| IdentityCenter:group:describe                | Grants permission to query group details.                      | Read         | -                           | -             | -     |
| IdentityCenter:group:describeGroups          | Grants permission to batch obtain group details.               | Read         | -                           | -             | -     |
| IdentityCenter:group:update                  | Grants permission to update a group.                           | Write        | -                           | -             | -     |
| IdentityCenter:group:delete                  | Grants permission to delete a group.                           | Write        | -                           | -             | -     |
| IdentityCenter:group:getGroupID              | Grants permission to obtain the group ID.                      | Read         | -                           | -             | -     |
| IdentityCenter:groupMembership:create        | Grants permission to add a member to a group.                  | Write        | -                           | -             | -     |
| IdentityCenter:groupMemberships:list         | Grants permission to query all members in a group.             | Read         | -                           | -             | -     |
| IdentityCenter:groupMembership:listForMember | Grants permission to query all groups that a user is added to. | Read         | -                           | -             | -     |

| Action                                              | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:groupMembership:describe             | Grants permission to query the group membership.                                                 | Read         | -                           | -             | -     |
| IdentityCenter:groupMembership:delete               | Grants permission to disassociate users and groups.                                              | Write        | -                           | -             | -     |
| IdentityCenter:groupMembership:getGroupMembershipId | Grants permission to query the membership ID.                                                    | Read         | -                           | -             | -     |
| IdentityCenter:groupMembership:isMembershipInGroup  | Grants permission to query whether a user is in a group.                                         | Read         | -                           | -             | -     |
| IdentityCenter:externalIdp:create                   | Grants permission to create an external identity provider.                                       | Write        | -                           | -             | -     |
| IdentityCenter:externalIdp:list                     | Grants permission to obtain the identity source configuration of the external identity provider. | Read         | -                           | -             | -     |

| Action                                       | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:externaldp:enable             | Grants permission to enable an external identity provider.                                 | Write        | -                           | -             | -     |
| IdentityCenter:externaldp:disable            | Grants permission to disable an external identity provider.                                | Write        | -                           | -             | -     |
| IdentityCenter:externaldp:getSpConfiguration | Grants permission to obtain the configuration of the IAM Identity Center service provider. | Read         | -                           | -             | -     |
| IdentityCenter:externaldp:update             | Grants permission to update the configuration of the external identity provider.           | Write        | -                           | -             | -     |
| IdentityCenter:externaldp:delete             | Grants permission to delete the configuration of the external identity provider.           | Write        | -                           | -             | -     |
| IdentityCenter:externaldp:importCertificate  | Grants permission to import a certificate.                                                 | Write        | -                           | -             | -     |



| Action                                              | Description                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------------------|---------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:externalldp:deleteCertificate        | Grants permission to delete a certificate.        | Write        | -                           | -             | -     |
| IdentityCenter:externalldp:listCertificates         | Grants permission to obtain the certificate list. | Read         | -                           | -             | -     |
| IdentityCenter:externalldp:createProvisioningTenant | Grants permission to create a tenant.             | Write        | -                           | -             | -     |
| IdentityCenter:externalldp:listProvisioningTenant   | Grants permission to query the tenant list.       | Read         | -                           | -             | -     |
| IdentityCenter:externalldp:deleteProvisioningTenant | Grants permission to delete a tenant.             | Write        | -                           | -             | -     |
| IdentityCenter:externalldp:createBearerToken        | Grants permission to create a bearer token.       | Write        | -                           | -             | -     |
| IdentityCenter:externalldp:listBearerTokens         | Grants permission to query the bearer token list. | Read         | -                           | -             | -     |
| IdentityCenter:externalldp:deleteBearerToken        | Grants permission to delete a bearer token.       | Write        | -                           | -             | -     |

| Action                                       | Description                                                                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:user:updatePassword           | Grants permission to update a password by sending a password reset link via email or generating a one-time password for a user. | Write        | -                           | -             | -     |
| IdentityCenter:user:deleteUserMfaDevice      | Grants permission to delete an MFA device for a specified user.                                                                 | Write        | -                           | -             | -     |
| IdentityCenter:user:updateMfaDevice          | Grants permission to update MFA device information.                                                                             | Write        | -                           | -             | -     |
| IdentityCenter:user:listMfaDevice            | Grants permission to query the MFA device list.                                                                                 | Read         | -                           | -             | -     |
| IdentityCenter:user:registerVirtualMfaDevice | Grants permission to begin the creation process of a virtual MFA device.                                                        | Write        | -                           | -             | -     |
| IdentityCenter:user:verifyEmail              | Grants permission to verify an email address of a user.                                                                         | Write        | -                           | -             | -     |

| Action                                             | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:user:batchDeleteSession             | Grants permission to delete user sessions in batches.         | Write        | -                           | -             | -     |
| IdentityCenter:user:listSessions                   | Grants permission to query the user session list.             | List         | -                           | -             | -     |
| IdentityCenter:serviceProvider:activateCertificate | Grants permission to activate identity provider certificates. | Write        | -                           | -             | -     |
| IdentityCenter:serviceProvider:deleteCertificate   | Grants permission to delete identity provider certificates.   | Write        | -                           | -             | -     |
| IdentityCenter:serviceProvider:createCertificate   | Grants permission to create identity provider certificates.   | Write        | -                           | -             | -     |
| IdentityCenter:serviceProvider:listCertificates    | Grants permission to obtain identity provider certificates.   | List         | -                           | -             | -     |
| IdentityCenter:permissionSet:create                | Grants permission to create a permission set.                 | Write        | instance *                  | -             | -     |
|                                                    |                                                               |              | permission Set *            | -             |       |

| Action                                           | Description                                                                          | Access Level          | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|--------------------------------------------------|--------------------------------------------------------------------------------------|-----------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                                  |                                                                                      |                       | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| IdentityCenter:permissionSet:attachManagedPolicy | Grants permission to attach system-defined policies to a permission set.             | Permission management | instance *                  | -                                                                                                                                     | -     |
|                                                  |                                                                                      |                       | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         |       |
| IdentityCenter:permissionSet:detachManagedPolicy | Grants permission to detach system-defined policies from a specified permission set. | Permission management | instance *                  | -                                                                                                                                     | -     |
|                                                  |                                                                                      |                       | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         |       |
| IdentityCenter:permissionSet:update              | Grants permission to update the permission set of a specified instance.              | Permission management | instance *                  | -                                                                                                                                     | -     |
|                                                  |                                                                                      |                       | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         |       |
| IdentityCenter:permissionSet:delete              | Grants permission to delete the permission set of a specified instance.              | Write                 | instance *                  | -                                                                                                                                     | -     |
|                                                  |                                                                                      |                       | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         |       |
| IdentityCenter:permissionSet:list                | Grants permission to list the permission sets of a specified instance.               | List                  | instance *                  | -                                                                                                                                     | -     |

| Action                                                  | Description                                                                                             | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| IdentityCenter:permissionSet:listAccountsForProvisioned | Grants permission to list all the accounts that the specified permission set is associated with.        | List         | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
|                                                         |                                                                                                         |              | instance *                  | -                                             |       |
| IdentityCenter:permissionSet:listProvisioningStatus     | Grants permission to list the status of the permission set attachment request for a specified instance. | List         | instance *                  | -                                             | -     |
| IdentityCenter:permissionSet:listManagedPolicies        | Grants permission to list the system-defined policies attached to a specified permission set.           | List         | instance *                  | -                                             | -     |
|                                                         |                                                                                                         |              | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:permissionSet:listProvisionedToAccount   | Grants permission to list all permission sets associated with a specified account.                      | List         | account *                   | -                                             | -     |
|                                                         |                                                                                                         |              | instance *                  | -                                             |       |
| IdentityCenter:permissionSet:describeProvisioningStatus | Grants permission to obtain the details of the permission set attachment status.                        | Read         | instance *                  | -                                             | -     |

| Action                                            | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|---------------------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| IdentityCenter:permissionSet:describe             | Grants permission to obtain the permission set details of a specified instance.  | Read         | instance *                  | -                                             |       |
|                                                   |                                                                                  |              | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:permissionSet:provision            | Grants permission to attach a specified permission set to a specified principal. | Write        | account *                   | -                                             |       |
|                                                   |                                                                                  |              | instance *                  | -                                             |       |
|                                                   |                                                                                  |              | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:instance:getIdentityCenterStatus   | Grants permission to query the IAM Identity Center service status.               | Read         | -                           | -                                             | -     |
| IdentityCenter:instance:registerRegion            | Grants permission to register a region.                                          | Write        | -                           | -                                             | -     |
| IdentityCenter:instance:describeRegisteredRegions | Grants permission to query regions enabled in IAM Identity Center.               | Read         | -                           | -                                             | -     |
| IdentityCenter:instance:startIdentityCenter       | Grants permission to enable IAM Identity Center.                                 | Write        | -                           | -                                             | -     |
| IdentityCenter:instance:deleteIdentityCenter      | Grants permission to disable IAM Identity Center.                                | Write        | -                           | -                                             | -     |

| Action                                                                      | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| IdentityCenter:instance:list                                                | Grants permission to query the IAM Identity Center instance list.              | List         | -                           | -                                             | -     |
| IdentityCenter:instance:describeInstanceAccessControlAttributeConfiguration | Grants permission to query access control attributes of a specific instance.   | Read         | instance *                  | -                                             | -     |
| IdentityCenter:instance:updateInstanceAccessControlAttributeConfiguration   | Grants permission to update access control attributes of a specific instance.  | Write        | instance *                  | -                                             | -     |
| IdentityCenter:instance:deleteInstanceAccessControlAttributeConfiguration   | Grants permission to delete access control attributes of a specific instance.  | Write        | instance *                  | -                                             | -     |
| IdentityCenter:instance:createInstanceAccessControlAttributeConfiguration   | Grants permission to enable access control attributes for a specific instance. | Write        | instance *                  | -                                             | -     |
| IdentityCenter:tags:list                                                    | Grants permission to list the tags attached to a specific resource.            | List         | instance *                  | -                                             | -     |
|                                                                             |                                                                                |              | permission Set              | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |

| Action                                  | Description                                                                                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| IdentityCenter:resources:tag            | Grants permission to add tags to a specific resource.                                                       | Tagging      | instance *                  | -                                                                                                                                 | -     |
|                                         |                                                                                                             |              | permission Set              | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                                         |                                                                                                             |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| IdentityCenter:resources:untag          | Grants permission to delete tags from a specific resource.                                                  | Tagging      | instance *                  | -                                                                                                                                 | -     |
|                                         |                                                                                                             |              | permission Set              | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
|                                         |                                                                                                             |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| IdentityCenter:accountAssignment:create | Grants permission to assign access to principals for a specified account using a specified permission set.  | Write        | instance *                  | -                                                                                                                                 | -     |
|                                         |                                                                                                             |              | account *                   | -                                                                                                                                 |       |
|                                         |                                                                                                             |              | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |
| IdentityCenter:accountAssignment:delete | Grants permission to delete a principal's access from a specified account using a specified permission set. | Write        | instance *                  | -                                                                                                                                 | -     |
|                                         |                                                                                                             |              | account *                   | -                                                                                                                                 |       |
|                                         |                                                                                                             |              | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |       |



| Action                                                  | Description                                                                                                                   | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| IdentityCenter:accountAssignment:list                   | Grants permission to list the assignee of the specified account with the specified permission set.                            | List         | instance *                  | -                                             | -     |
|                                                         |                                                                                                                               |              | account *                   | -                                             |       |
|                                                         |                                                                                                                               |              | permission Set *            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:accountAssignment:describeDeletionStatus | Grants permission to obtain the details about the status of the assignment deletion request.                                  | Read         | instance *                  | -                                             | -     |
| IdentityCenter:accountAssignment:describeCreationStatus | Grants permission to obtain the details about the status of the assignment creation request.                                  | Read         | instance *                  | -                                             | -     |
| IdentityCenter:accountAssignment:listCreationStatus     | Grants permission to list the status of the account assignment creation request for a specified IAM Identity Center instance. | List         | instance *                  | -                                             | -     |

| Action                                                 | Description                                                                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:accountAssignment:listDeletionStatus    | Grants permission to list the status of the account assignment deletion request for a specified IAM Identity Center instance. | List         | instance *                  | -             | -     |
| IdentityCenter:accountAssignment:disassociationProfile | Grants permission to disassociate all authorizations from a user or group.                                                    | Write        | -                           | -             | -     |
| IdentityCenter:instance:listIdentityStoreAssociations  | Grants permission to query details about the identity source configured in IAM Identity Center.                               | Read         | -                           | -             | -     |
| IdentityCenter:ssoConfiguration:update                 | Grants permission to update the configuration for the current IAM Identity Center instance.                                   | Write        | -                           | -             | -     |

| Action                                               | Description                                                                                 | Access Level          | Resource Type (*: required) | Condition Key                                 | Alias |
|------------------------------------------------------|---------------------------------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------|-------|
| IdentityCenter:ssoConfiguration:describe             | Grants permission to obtain the configuration for the current IAM Identity Center instance. | Read                  | -                           | -                                             | -     |
| IdentityCenter:mfaDevices:describeManagementSettings | Grants permission to obtain MFA settings.                                                   | Read                  | -                           | -                                             | -     |
| IdentityCenter:mfaDevices:updateManagementSettings   | Grants permission to update MFA settings.                                                   | Write                 | -                           | -                                             | -     |
| IdentityCenter:instance:createAlias                  | Grants permission to create an alias for a specified identity source.                       | Write                 | -                           | -                                             | -     |
| IdentityCenter:permissionSet:attachCustomRole        | Grants permission to attach a custom role to a permission set.                              | Permission_management | instance *                  | -                                             | -     |
|                                                      |                                                                                             |                       | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:permissionSet:attachCustomPolicy      | Grants permission to attach a custom policy to a permission set.                            | Permission_management | instance *                  | -                                             | -     |
|                                                      |                                                                                             |                       | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |

| Action                                                          | Description                                                              | Access Level          | Resource Type (*: required) | Condition Key                                 | Alias |
|-----------------------------------------------------------------|--------------------------------------------------------------------------|-----------------------|-----------------------------|-----------------------------------------------|-------|
| IdentityCenter:permissionSet:getCustomRole                      | Grants permission to obtain a custom role of a permission set.           | Read                  | instance *                  | -                                             |       |
|                                                                 |                                                                          |                       | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:permissionSet:getCustomPolicy                    | Grants permission to obtain a custom policy of a permission set.         | Read                  | instance *                  | -                                             |       |
|                                                                 |                                                                          |                       | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:permissionSet:detachCustomRole                   | Grants permission to delete a custom role of a permission set.           | Permission management | instance *                  | -                                             |       |
|                                                                 |                                                                          |                       | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:permissionSet:detachCustomPolicy                 | Grants permission to delete a custom policy of a permission set.         | Permission management | instance *                  | -                                             |       |
|                                                                 |                                                                          |                       | permissionSet *             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |       |
| IdentityCenter:application:createApplicationInstance            | Grants permission to add an application instance to IAM Identity Center. | Write                 | -                           | -                                             | -     |
| IdentityCenter:application:createApplicationInstanceCertificate | Grants permission to add a new certificate for an application instance.  | Write                 | -                           | -                                             | -     |

| Action                                                           | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:application:deleteApplicationInstance             | Grants permission to delete the application instance.                                                 | Write        | -                           | -             | -     |
| IdentityCenter:application:deleteApplicationInstanceCertificate  | Grants permission to delete an inactive or expired certificate from the application instance.         | Write        | -                           | -             | -     |
| IdentityCenter:application:deleteProfile                         | Grants permission to delete the association between an application instance and a user or user group. | Write        | -                           | -             | -     |
| IdentityCenter:application:describeApplication                   | Grants permission to obtain information about an application.                                         | Read         | application *               | -             | -     |
| IdentityCenter:application:getApplicationAssignmentConfiguration | Grants permission to read assignment configurations for an application.                               | Read         | application *               | -             | -     |
| IdentityCenter:application:getApplicationInstance                | Grants permission to retrieve details for an application instance.                                    | Read         | -                           | -             | -     |

| Action                                                                      | Description                                                                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:application:importApplicationInstanceServiceProviderMetadata | Grants permission to update the application instance by uploading an application SAML metadata file provided by the service provider. | Write        | -                           | -             | -     |
| IdentityCenter:application:listApplicationInstanceCertificates              | Grants permission to retrieve all of the certificates for a given application instance.                                               | List         | -                           | -             | -     |
| IdentityCenter:application:listApplicationInstances                         | Grants permission to retrieve all application instances.                                                                              | List         | -                           | -             | -     |
| IdentityCenter:application:listApplicationTemplates                         | Grants permission to retrieve all supported application templates.                                                                    | List         | -                           | -             | -     |
| IdentityCenter:application:listApplications                                 | Grants permission to retrieve all applications associated with the instance of IAM Identity Center.                                   | List         | -                           | -             | -     |

| Action                                                                          | Description                                                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:application:listProfiles                                         | Grants permission to check whether an application instance is associated with a user or user group. | List         | -                           | -             | -     |
| IdentityCenter:application:updateApplicationInstanceActiveCertificate           | Grants permission to set a certificate as the active one for this application instance.             | Write        | -                           | -             | -     |
| IdentityCenter:application:updateApplicationInstanceDisplayData                 | Grants permission to update the display details of an application instance.                         | Write        | -                           | -             | -     |
| IdentityCenter:application:updateApplicationInstanceResponseConfiguration       | Grants permission to update federation response configuration for the application instance.         | Write        | -                           | -             | -     |
| IdentityCenter:application:updateApplicationInstanceResponseSchemaConfiguration | Grants permission to update federation response schema configuration for the application instance.  | Write        | -                           | -             | -     |

| Action                                                                           | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:application:updateApplicationInstanceSecurityConfiguration        | Grants permission to update the security configurations of an application instance.              | Write        | -                           | -             | -     |
| IdentityCenter:application:updateApplicationInstanceServiceProviderConfiguration | Grants permission to update service provider related configuration for the application instance. | Write        | -                           | -             | -     |
| IdentityCenter:application:updateApplicationInstanceStatus                       | Grants permission to update the status of an application instance.                               | Write        | -                           | -             | -     |
| IdentityCenter:applicationProvider:describeApplicationProvider                   | Grants permission to describe an application provider.                                           | Read         | application Provider *      | -             | -     |
| IdentityCenter:applicationProvider:listApplicationProviders                      | Grants permission to list application providers.                                                 | List         | application Provider        | -             | -     |
| IdentityCenter:applicationAssignment:create                                      | Grants permission to create an application assignment.                                           | Write        | application *               | -             | -     |



| Action                                                 | Description                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| IdentityCenter:applicationAssignment:delete            | Grants permission to delete an application assignment.            | Write        | application *               | -             | -     |
| IdentityCenter:applicationAssignment:list              | Grants permission to list application assignments.                | List         | application *               | -             | -     |
| IdentityCenter:applicationAssignmentsForPrincipal:list | Grants permission to list applications assigned to user or group. | List         | instance *                  | -             | -     |

Each API of IdentityCenter usually supports one or more actions. [Table 3-252](#) lists the supported actions and dependencies.

**Table 3-252** Actions and dependencies supported by IdentityCenter APIs

| API                                                            | Action                             | Dependencies                               |
|----------------------------------------------------------------|------------------------------------|--------------------------------------------|
| POST /v1/identity-stores/{identity_store_id}/users             | IdentityCenter:user:create         | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/users              | IdentityCenter:user:list           | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/users/{user_id}    | IdentityCenter:user:describe       | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/batch-query | IdentityCenter:user:describe Users | organizations:delegatedAdministrators:list |

| API                                                                  | Action                              | Dependencies                               |
|----------------------------------------------------------------------|-------------------------------------|--------------------------------------------|
| PUT /v1/identity-stores/{identity_store_id}/users/{user_id}          | IdentityCenter:user:update          | organizations:delegatedAdministrators:list |
| DELETE /v1/identity-stores/{identity_store_id}/users/{user_id}       | IdentityCenter:user:delete          | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/retrieve-user-id  | IdentityCenter:user:getUserId       | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/{user_id}/enable  | IdentityCenter:user:enableUser      | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/{user_id}/disable | IdentityCenter:user:disableUser     | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/groups                  | IdentityCenter:group:create         | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/groups                   | IdentityCenter:group:list           | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/groups/{group_id}        | IdentityCenter:group:describe       | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/groups/batch-query      | IdentityCenter:group:describeGroups | organizations:delegatedAdministrators:list |
| PUT /v1/identity-stores/{identity_store_id}/groups/{group_id}        | IdentityCenter:group:update         | organizations:delegatedAdministrators:list |

| API                                                                                         | Action                                              | Dependencies                               |
|---------------------------------------------------------------------------------------------|-----------------------------------------------------|--------------------------------------------|
| DELETE /v1/identity-stores/{identity_store_id}/groups/{group_id}                            | IdentityCenter:group:delete                         | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/groups/retrieve-group-id                       | IdentityCenter:group:getGroupId                     | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/group-memberships                              | IdentityCenter:groupMembership:create               | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/group-memberships                               | IdentityCenter:groupMembership:list                 | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/group-memberships-for-member                    | IdentityCenter:groupMembership:listForMember        | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}               | IdentityCenter:groupMembership:describe             | organizations:delegatedAdministrators:list |
| DELETE /v1/identity-stores/{identity_store_id}/group-memberships/{membership_id}            | IdentityCenter:groupMembership:delete               | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/group-memberships/retrieve-group-membership-id | IdentityCenter:groupMembership:getGroupMembershipId | organizations:delegatedAdministrators:list |

| API                                                                            | Action                                             | Dependencies                               |
|--------------------------------------------------------------------------------|----------------------------------------------------|--------------------------------------------|
| POST /v1/identity-stores/{identity_store_id}/iss-member-in-groups              | IdentityCenter:groupMembership:isMembershipInGroup | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/external-idp                      | IdentityCenter:externalIdp:create                  | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/external-idp                       | IdentityCenter:externalIdp:list                    | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/enable      | IdentityCenter:externalIdp:enable                  | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/disable     | IdentityCenter:externalIdp:disable                 | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/ssp-config                         | IdentityCenter:externalIdp:getSpConfiguration      | organizations:delegatedAdministrators:list |
| PUT /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}              | IdentityCenter:externalIdp:update                  | organizations:delegatedAdministrators:list |
| DELETE /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}           | IdentityCenter:externalIdp:delete                  | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate | IdentityCenter:externalIdp:importCertificate       | organizations:delegatedAdministrators:list |

| API                                                                                               | Action                                              | Dependencies                               |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------|--------------------------------------------|
| DELETE /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate/{certificate_id} | IdentityCenter:externalIdp:deleteCertificate        | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/external-idp/{idp_id}/certificate                     | IdentityCenter:externalIdp:listCertificates         | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/provision-tenant                                     | IdentityCenter:externalIdp:createProvisioningTenant | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/provision-tenant                                      | IdentityCenter:externalIdp:listProvisioningTenant   | organizations:delegatedAdministrators:list |
| DELETE /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}                                 | IdentityCenter:externalIdp:deleteProvisioningTenant | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token                      | IdentityCenter:externalIdp:createBearerToken        | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token                       | IdentityCenter:externalIdp:listBearerTokens         | organizations:delegatedAdministrators:list |
| DELETE /v1/identity-stores/{identity_store_id}/tenant/{tenant_id}/bearer-token/{token_id}         | IdentityCenter:externalIdp:deleteBearerToken        | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/{user_id}/reset-password                       | IdentityCenter:user:updatePassword                  | organizations:delegatedAdministrators:list |

| API                                                                                          | Action                                           | Dependencies                               |
|----------------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------|
| DELETE /v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/{device_id}       | IdentityCenter:user:deleteUserMfaDevice          | organizations:delegatedAdministrators:list |
| PUT /v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/{device_id}          | IdentityCenter:user:updateMfaDevice              | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/retrieve-mfa-devices                      | IdentityCenter:user:listMfaDevice                | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/{user_id}/mfa-devices/register-mfa-device | IdentityCenter:user:registerVirtualMfaDevice     | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/{user_id}/verify-email                    | IdentityCenter:user:verifyEmail                  | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/users/{user_id}/sessions/batch-delete           | IdentityCenter:user:batchDeleteSession           | organizations:delegatedAdministrators:list |
| GET /v1/identity-stores/{identity_store_id}/users/{user_id}/sessions                         | IdentityCenter:user:listSessions                 | organizations:delegatedAdministrators:list |
| POST /v1/identity-stores/{identity_store_id}/saml-certificates                               | IdentityCenter:serviceProvider:createCertificate | organizations:delegatedAdministrators:list |

| API                                                                                        | Action                                           | Dependencies                                                                                                             |
|--------------------------------------------------------------------------------------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| DELETE /v1/identity-stores/{identity_store_id}/saml-certificates/{certificate_id}          | IdentityCenter:serviceProvider:deleteCertificate | organizations:delegatedAdministrators:list                                                                               |
| GET /v1/identity-stores/{identity_store_id}/saml-certificates                              | IdentityCenter:serviceProvider:listCertificates  | organizations:delegatedAdministrators:list                                                                               |
| POST /v1/identity-stores/{identity_store_id}/saml-certificates/{certificate_id}/active     | IdentityCenter:serviceProvider:activeCertificate | organizations:delegatedAdministrators:list                                                                               |
| POST /v1/instances/{instance_id}/permission-sets                                           | IdentityCenter:permissionSet:create              | organizations:delegatedAdministrators:list                                                                               |
| POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/attach-managed-policy | IdentityCenter:permissionSet:attachManagedPolicy | <ul style="list-style-type: none"> <li>iam:policies:getV5</li> <li>organizations:delegatedAdministrators:list</li> </ul> |
| POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/detach-managed-policy | IdentityCenter:permissionSet:detachManagedPolicy | organizations:delegatedAdministrators:list                                                                               |
| PUT /v1/instances/{instance_id}/permission-sets/{permission_set_id}                        | IdentityCenter:permissionSet:update              | organizations:delegatedAdministrators:list                                                                               |
| DELETE /v1/instances/{instance_id}/permission-sets/{permission_set_id}                     | IdentityCenter:permissionSet:delete              | organizations:delegatedAdministrators:list                                                                               |
| GET /v1/instances/{instance_id}/permission-sets                                            | IdentityCenter:permissionSet:list                | organizations:delegatedAdministrators:list                                                                               |

| API                                                                                  | Action                                                  | Dependencies                               |
|--------------------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------|
| GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/accounts         | IdentityCenter:permissionSet:listAccountsForProvisioned | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/permission-sets/provisioning-statuses                | IdentityCenter:permissionSet:listProvisioningStatus     | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/managed-policies | IdentityCenter:permissionSet:listManagedPolicies        | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/permission-sets/provisioned-to-accounts              | IdentityCenter:permissionSet:listProvisionedToAccount   | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/permission-sets/provisioning-status/{request_id}     | IdentityCenter:permissionSet:describeProvisioningStatus | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}                  | IdentityCenter:permissionSet:describe                   | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/permission-sets/{permission_set_id}/provision       | IdentityCenter:permissionSet:provision                  | organizations:delegatedAdministrators:list |
| GET /v1/identity-center-service/status                                               | IdentityCenter:instance:getIdentityCenterStatus         | organizations:delegatedAdministrators:list |
| POST /v1/register-regions                                                            | IdentityCenter:instance:registerRegion                  | -                                          |
| GET /v1/registered-regions                                                           | IdentityCenter:instance:describeRegisteredRegions       | organizations:delegatedAdministrators:list |



| API                                                                       | Action                                                                      | Dependencies                                                                                                                           |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/service/start                                                    | IdentityCenter:instance:startIdentityCenter                                 | <ul style="list-style-type: none"> <li>iam:agencies:createServiceLinkedAgency</li> <li>organizations:trustedServices:enable</li> </ul> |
| POST /v1/service/delete                                                   | IdentityCenter:instance:deleteIdentityCenter                                | iam:agencies:deleteServiceLinkedAgency                                                                                                 |
| GET /v1/instances                                                         | IdentityCenter:instance:list                                                | organizations:delegatedAdministrators:list                                                                                             |
| GET /v1/instances/{instance_id}/access-control-attribute-configuration    | IdentityCenter:instance:describeInstanceAccessControlAttributeConfiguration | organizations:delegatedAdministrators:list                                                                                             |
| PUT /v1/instances/{instance_id}/access-control-attribute-configuration    | IdentityCenter:instance:updateInstanceAccessControlAttributeConfiguration   | organizations:delegatedAdministrators:list                                                                                             |
| DELETE /v1/instances/{instance_id}/access-control-attribute-configuration | IdentityCenter:instance:deleteInstanceAccessControlAttributeConfiguration   | organizations:delegatedAdministrators:list                                                                                             |
| POST /v1/instances/{instance_id}/access-control-attribute-configuration   | IdentityCenter:instance:createInstanceAccessControlAttributeConfiguration   | organizations:delegatedAdministrators:list                                                                                             |
| GET /v1/instances/{resource_type}/{resource_id}/tags                      | IdentityCenter:tags:list                                                    | organizations:delegatedAdministrators:list                                                                                             |
| POST /v1/instances/{resource_type}/{resource_id}/tags/create              | IdentityCenter:resources:tag                                                | organizations:delegatedAdministrators:list                                                                                             |
| POST /v1/instances/{resource_type}/{resource_id}/tags/delete              | IdentityCenter:resources:untag                                              | organizations:delegatedAdministrators:list                                                                                             |

| API                                                                              | Action                                                  | Dependencies                               |
|----------------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------|
| POST /v1/instances/{instance_id}/account-assignments/create                      | IdentityCenter:accountAssignment:create                 | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/account-assignments/delete                      | IdentityCenter:accountAssignment:delete                 | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/account-assignments                              | IdentityCenter:accountAssignment:list                   | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/account-assignments/deletion-status/{request_id} | IdentityCenter:accountAssignment:describeDeletionStatus | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/account-assignments/creation-status/{request_id} | IdentityCenter:accountAssignment:describeCreationStatus | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/account-assignments/creation-statuses            | IdentityCenter:accountAssignment:listCreationStatus     | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/account-assignments/deletion-statuses            | IdentityCenter:accountAssignment:listDeletionStatus     | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/disassociate-profile                            | IdentityCenter:accountAssignment:disassociationProfile  | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/identity-store-associations                      | IdentityCenter:instance:listIdentityStoreAssociations   | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/sso-configuration                               | IdentityCenter:ssoConfiguration:update                  | organizations:delegatedAdministrators:list |

| API                                                                                  | Action                                               | Dependencies                               |
|--------------------------------------------------------------------------------------|------------------------------------------------------|--------------------------------------------|
| GET /v1/instances/{instance_id}/sso-configuration                                    | IdentityCenter:ssoConfiguration:describe             | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/mfa-devices/management-settings                      | IdentityCenter:mfaDevices:describeManagementSettings | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/mfa-devices/management-settings                     | IdentityCenter:mfaDevices:updateManagementSettings   | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/alias                                               | IdentityCenter:instance:createAlias                  | organizations:delegatedAdministrators:list |
| DELETE /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy | IdentityCenter:permissionSet:detachCustomPolicy      | organizations:delegatedAdministrators:list |
| DELETE /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-role   | IdentityCenter:permissionSet:detachCustomRole        | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy    | IdentityCenter:permissionSet:getCustomPolicy         | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-role      | IdentityCenter:permissionSet:getCustomRole           | organizations:delegatedAdministrators:list |
| PUT /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-policy    | IdentityCenter:permissionSet:attachCustomPolicy      | organizations:delegatedAdministrators:list |

| API                                                                                                              | Action                                                           | Dependencies                               |
|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|--------------------------------------------|
| PUT /v1/instances/{instance_id}/permission-sets/{permission_set_id}/custom-role                                  | IdentityCenter:permissionSet:attachCustomRole                    | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/application-instances                                                           | IdentityCenter:application:createApplicationInstance             | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates                    | IdentityCenter:application:createApplicationInstance-Certificate | organizations:delegatedAdministrators:list |
| DELETE /v1/instances/{instance_id}/application-instances/{application_instance_id}                               | IdentityCenter:application:deleteApplicationInstance             | organizations:delegatedAdministrators:list |
| DELETE /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates/{certificate_id} | IdentityCenter:application:deleteApplicationInstance-Certificate | organizations:delegatedAdministrators:list |
| DELETE /v1/instances/{instance_id}/application-instances/{application_instance_id}/profiles/{profile_id}         | IdentityCenter:application:deleteProfile                         | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/applications/{application_instance_id}                                           | IdentityCenter:application:describeApplication                   | organizations:delegatedAdministrators:list |

| API                                                                                              | Action                                                                       | Dependencies                                                                                                                                            |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1/instances/{instance_id}/applications/{application_instance_id}/assignments-configuration | IdentityCenter:application:getApplicationAssignment-Configuration            | organizations:delegatedAdministrators:list                                                                                                              |
| GET /v1/instances/{instance_id}/application-instances/{application_instance_id}                  | IdentityCenter:application:getApplicationInstance                            | organizations:delegatedAdministrators:list                                                                                                              |
| POST /v1/instances/{instance_id}/application-instances/{application_instance_id}/metadata        | IdentityCenter:application:importApplicationInstance-ServiceProviderMetadata | organizations:delegatedAdministrators:list                                                                                                              |
| GET /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates     | IdentityCenter:application:listApplicationInstanceCertificates               | organizations:delegatedAdministrators:list                                                                                                              |
| GET /v1/instances/{instance_id}/application-instances                                            | IdentityCenter:application:listApplicationInstances                          | <ul style="list-style-type: none"> <li>organizations:delegatedAdministrators:list</li> <li>IdentityCenter:application:getApplicationInstance</li> </ul> |
| GET /v1/application-templates                                                                    | IdentityCenter:application:listApplicationTemplates                          | organizations:delegatedAdministrators:list                                                                                                              |
| GET /v1/instances/{instance_id}/applications                                                     | IdentityCenter:application:listApplications                                  | organizations:delegatedAdministrators:list                                                                                                              |
| GET /v1/instances/{instance_id}/application-instances/{application_instance_id}/profiles         | IdentityCenter:application:listProfiles                                      | organizations:delegatedAdministrators:list                                                                                                              |

| API                                                                                                            | Action                                                                           | Dependencies                               |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------|
| PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/certificates/{certificate_id}  | IdentityCenter:application:updateApplicationInstanceActiveCertificate            | organizations:delegatedAdministrators:list |
| PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/display-data                   | IdentityCenter:application:updateApplicationInstanceDisplayData                  | organizations:delegatedAdministrators:list |
| PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/response-configuration         | IdentityCenter:application:updateApplicationInstanceResponseConfiguration        | organizations:delegatedAdministrators:list |
| PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/response-schema-configuration  | IdentityCenter:application:updateApplicationInstanceResponseSchemaConfiguration  | organizations:delegatedAdministrators:list |
| PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/security-configuration         | IdentityCenter:application:updateApplicationInstanceSecurityConfiguration        | organizations:delegatedAdministrators:list |
| PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/service-provider-configuration | IdentityCenter:application:updateApplicationInstanceServiceProviderConfiguration | organizations:delegatedAdministrators:list |

| API                                                                                        | Action                                                         | Dependencies                               |
|--------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------|
| PUT /v1/instances/{instance_id}/application-instances/{application_instance_id}/status     | IdentityCenter:application:updateApplicationInstanceStatus     | organizations:delegatedAdministrators:list |
| GET /v1/application-providers/{application_provider_id}                                    | IdentityCenter:applicationProvider:describeApplicationProvider | organizations:delegatedAdministrators:list |
| GET /v1/application-providers                                                              | IdentityCenter:applicationProvider:listApplicationProviders    | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/applications/{application_instance_id}/assignments/create | IdentityCenter:applicationAssignment:create                    | organizations:delegatedAdministrators:list |
| POST /v1/instances/{instance_id}/applications/{application_instance_id}/assignments/delete | IdentityCenter:applicationAssignment:delete                    | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/applications/{application_instance_id}/assignments         | IdentityCenter:applicationAssignment:list                      | organizations:delegatedAdministrators:list |
| GET /v1/instances/{instance_id}/application-assignments-for-principals                     | IdentityCenter:applicationAssignmentsForPrincipal:list         | organizations:delegatedAdministrators:list |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-253](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all

resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for IdentityCenter.

**Table 3-253** Resource types supported by IdentityCenter

| Resource Type       | URN                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------|
| application         | IdentityCenter::<management-account-id>:application:<instance-id>/<application-instance-id> |
| account             | IdentityCenter::<management-account-id>:account:<account-id>                                |
| instance            | IdentityCenter::<management-account-id>:instance:<instance-id>                              |
| permissionSet       | IdentityCenter::<management-account-id>:permissionSet:<instance-id>/<permission-set-id>     |
| applicationProvider | IdentityCenter:::applicationProvider:<application-provider-name>                            |

## Conditions

IdentityCenter does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.14.5 Resource Management Service (RMS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).



- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by Config, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Config, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Config.

**Table 3-254** Actions supported by Config

| Action                                  | Description                                                                         | Access Level | Resource Type (*: required)    | Condition Key | Alias |
|-----------------------------------------|-------------------------------------------------------------------------------------|--------------|--------------------------------|---------------|-------|
| rms:organizationConformancePacks:create | Grants permission to create organization conformancePack.                           | Write        | -                              | -             | -     |
| rms:organizationConformancePacks:get    | Grants permission to return the details of a specific organization conformancePack. | Read         | organizationConformancePacks * | -             | -     |
| rms:organizationConformancePacks:delete | Grants permission to delete organization conformancePack.                           | Write        | organizationConformancePacks * | -             | -     |
| rms:organizationConformancePacks:update | Grants permission to update organization conformancePack.                           | Write        | organizationConformancePacks * | -             | -     |
| rms:organizationConformancePacks:list   | Grants permission to return a list of organization conformancePack.                 | List         | -                              | -             | -     |
| rms:conformancePacks:create             | Grants permission to create conformancePack.                                        | Write        | -                              | -             | -     |

| Action                      | Description                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rms:conformancePacks:get    | Grants permission to return the details of a specific conformancePack. | Read         | conformancePacks *          | -             | -     |
| rms:conformancePacks:delete | Grants permission to delete conformancePack.                           | Write        | conformancePacks *          | -             | -     |
| rms:conformancePacks:update | Grants permission to update conformancePack.                           | Write        | conformancePacks *          | -             | -     |
| rms:conformancePacks:list   | Grants permission to return a list of conformancePacks.                | List         | -                           | -             | -     |
| rms:storedQueries:create    | Grants permission to save a new query.                                 | Write        | -                           | -             | -     |
| rms:storedQueries:update    | Grants permission to update an existing saved query.                   | Write        | storedQueries *             | -             | -     |
| rms:storedQueries:delete    | Grants permission to delete the stored query.                          | Write        | storedQueries *             | -             | -     |
| rms:storedQueries:get       | Grants permission to return the details of a specific stored query.    | Read         | storedQueries *             | -             | -     |

| Action                                | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|---------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| rms:storedQueries:list                | Grants permission to list the stored queries.                                             | List         | -                           | -                                                                                                                                     | -     |
| rms:policyAssignments:create          | Grants permission to create a policy assignments.                                         | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> | -     |
| rms:policyAssignments:update          | Grants permission to update a policy assignments.                                         | Write        | policy Assignments *        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -     |
|                                       |                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> |       |
| rms:policyAssignments:delete          | Grants permission to delete the specified policy assignment and all of its policy states. | Write        | policy Assignments *        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -     |
| rms:policyAssignments:get             | Grants permission to return details about your policy assignments.                        | Read         | policy Assignments *        | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -     |
| rms:organizationPolicyAssignments:put | Grants permission to create or update organization policy assignment.                     | Write        | -                           | -                                                                                                                                     | -     |

| Action                                   | Description                                                                                                                                          | Access Level | Resource Type (*: required)     | Condition Key                                 | Alias |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------------------------------|-----------------------------------------------|-------|
| rms:organizationPolicyAssignments:delete | Grants permission to delete the specified organization policy assignment and all of its policy states from all member accounts in that organization. | Write        | organizationPolicyAssignments * | -                                             | -     |
| rms:organizationPolicyAssignments:get    | Grants permission to return the details of a specific organization policy assignment.                                                                | Read         | organizationPolicyAssignments * | -                                             | -     |
| rms:organizationPolicyAssignments:list   | Grants permission to return a list of organization policy assignments.                                                                               | List         | -                               | -                                             | -     |
| rms:policyStates:runEvaluation           | Grants permission to evaluate your resources against the specified policy assignment.                                                                | Write        | policyAssignments               | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                  | Description                                                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------|------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rms:policyStates:update | Grants permission to be used by a FunctionGraph function to deliver evaluation results to RMS. | Write        | -                           | -             | -     |
| rms:aggregators:create  | Grants permission to create aggregators with the selected source accounts.                     | Write        | -                           | -             | -     |
| rms:aggregators:update  | Grants permission to update an existing aggregator.                                            | Write        | aggregators *               | -             | -     |
| rms:aggregators:delete  | Grants permission to delete the specified aggregator and remove aggregated resources.          | Write        | aggregators *               | -             | -     |
| rms:aggregators:list    | Grants permission to list the aggregators.                                                     | List         | -                           | -             | -     |
| rms:aggregators:get     | Grants permission to return the details of a specific aggregator.                              | Read         | aggregators *               | -             | -     |

| Action                                       | Description                                                                                                                                                       | Access Level | Resource Type (*: required)                     | Condition Key                                 | Alias |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------------------------------------------|-----------------------------------------------|-------|
| rms:aggregat<br>orResources:li<br>st         | Grants permission to list the aggregated resources.                                                                                                               | List         | -                                               | -                                             | -     |
| rms:aggregat<br>orResources:r<br>unQuery     | Grants permission to accept a resource query language (ResourceQL) SELECT command, performs the corresponding search, and returns aggregated resource properties. | List         | -                                               | -                                             | -     |
| rms:aggregat<br>orResources:g<br>et          | Grants permission to return the details of specified aggregated resources.                                                                                        | Read         | -                                               | -                                             | -     |
| rms:aggregati<br>onAuthorizati<br>ons:create | Grants permission to create aggregation authorizations , allows specified account to aggregate resources.                                                         | Write        | aggre<br>gatio<br>nAut<br>horiz<br>ation<br>s * | -                                             | -     |
|                                              |                                                                                                                                                                   |              | -                                               | <b>rms:Authoriz<br/>edAccountOr<br/>gPath</b> |       |

| Action                               | Description                                                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                                                                                              | Alias |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|-------|
| rms:aggregationAuthorizations:list   | Grants permission to list the aggregation authorizations.                                                                       | List         | -                           | -                                                                                                                          | -     |
| rms:aggregationAuthorizations:delete | Grants permission to delete the aggregation authorization.                                                                      | Write        | aggregationAuthorizations * | -                                                                                                                          | -     |
|                                      |                                                                                                                                 |              | -                           | <b>rms:AuthorizedAccountOrPath</b>                                                                                         |       |
| rms:aggregationRequests:delete       | Grants permission to delete the aggregation request.                                                                            | Write        | -                           | -                                                                                                                          | -     |
| rms:aggregationRequests:list         | Grants permission to list the aggregation requests.                                                                             | List         | -                           | -                                                                                                                          | -     |
| rms:trackerConfig:put                | Grants permission to add or update the tracker for starting record configurations of the resources you have selected to record. | Write        | -                           | <ul style="list-style-type: none"> <li><b>rms:TrackerBucketName</b></li> <li><b>rms:TrackerBucketPathPrefix</b></li> </ul> | -     |



| Action                    | Description                                                                                                              | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rms:trackerConfig:delete  | Grants permission to delete the tracker for stopping record configurations of the resources you have selected to record. | Write        | -                           | -             | -     |
| rms:trackerConfig:get     | Grants permission to return the detail of specified tracker.                                                             | Read         | -                           | -             | -     |
| rms:schemas:list          | Grants permission to return the list for RMS schemas for ResourceQL.                                                     | List         | -                           | -             | -     |
| rms:policyDefinitions:get | Grants permission to return the list for supported RMS managed policy definitions.                                       | List         | -                           | -             | -     |
| rms:resources:getHistory  | Grants permission to return history of configuration for the specified resource.                                         | List         | -                           | -             | -     |

| Action                    | Description                                                                                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias                     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| rms:resources:getRelation | Grants permission to list relations of resource.                                                                                                       | List         | -                           | -                                                                                                                                 | -                         |
| rms:resources:get         | Grants permission to return the details of specified resources.                                                                                        | Read         | -                           | -                                                                                                                                 | -                         |
| rms:resources:list        | Grants permission to return the list of all resources.                                                                                                 | List         | -                           | -                                                                                                                                 | -                         |
| rms:resources:runQuery    | Grants permission to accept a resource query language (ResourceQL) SELECT command, performs the corresponding search, and returns resource properties. | List         | -                           | -                                                                                                                                 | -                         |
| rms::tagResource          | Grants permission to associate the specified tags to a resource.                                                                                       | Tagging      | policy Assignments          | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | rms:resources:tagResource |
|                           |                                                                                                                                                        |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                           |

| Action                                                          | Description                                                                 | Access Level | Resource Type (*: required)    | Condition Key                                                                                                                     | Alias                             |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------|--------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| rms::unTagResource                                              | Grants permission to delete specified tags from a resource.                 | Tagging      | policy Assignments             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | rms:resources:unTagResource       |
|                                                                 |                                                                             |              | -                              | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                                   |
| rms::listTagsForResource                                        | Grants permission to list the tags for a resource.                          | List         | policy Assignments             | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | rms:resources:listTagsForResource |
| rms::listTags                                                   | Grants permission to list the tags for all resources in the specified type. | List         | -                              | -                                                                                                                                 | rms:resources:listTags            |
| rms::listResourcesByTag                                         | Grants permission to list or count resources by the specified tags.         | List         | -                              | <a href="#">g:TagKeys</a>                                                                                                         | rms:resources:listResourcesByTag  |
| rms:policyAssignmentsRemediation:putRemediationConfiguration    | Grants permission to Create PolicyAssignments Remediation Configurations.   | Write        | policy AssignmentsRemediation* | -                                                                                                                                 | -                                 |
| rms:policyAssignmentsRemediation:deleteRemediationConfiguration | Grants permission to delete PolicyAssignments Remediation Configurations.   | Write        | policy AssignmentsRemediation* | -                                                                                                                                 | -                                 |

| Action                                                            | Description                                                               | Access Level | Resource Type (*: required)     | Condition Key | Alias |
|-------------------------------------------------------------------|---------------------------------------------------------------------------|--------------|---------------------------------|---------------|-------|
| rms:policyAssignmentsRemediation:getRemediationConfiguration      | Grants permission to get PolicyAssignments Remediation Configuration s.   | Read         | policy AssignmentsRemediation * | -             | -     |
| rms:policyAssignmentsRemediation:runRemediation                   | Grants permission to run PolicyAssignments Remediation Configuration s.   | Write        | policy AssignmentsRemediation * | -             | -     |
| rms:policyAssignmentsRemediation:listRemediationExecutionStatuses | Grants permission to View PolicyAssignments Remediation Execution Status. | List         | policy AssignmentsRemediation * | -             | -     |
| rms:policyAssignmentsRemediation:createRemediationExceptions      | Grants permission to create PolicyAssignments Remediation Exceptions.     | Write        | policy AssignmentsRemediation * | -             | -     |
| rms:policyAssignmentsRemediation:deleteRemediationExceptions      | Grants permission to delete PolicyAssignments Remediation Exceptions.     | Write        | policy AssignmentsRemediation * | -             | -     |

| Action                                                     | Description                                                         | Access Level | Resource Type (*: required)   | Condition Key | Alias |
|------------------------------------------------------------|---------------------------------------------------------------------|--------------|-------------------------------|---------------|-------|
| rms:policyAssignmentsRemediation:listRemediationExceptions | Grants permission to View PolicyAssignments Remediation Exceptions. | List         | policyAssignmentsRemediation* | -             | -     |

Each API of Config usually supports one or more actions. [Table 3-255](#) lists the supported actions and dependencies.

**Table 3-255** Actions and dependencies supported by Config APIs

| API                                                                                                 | Action                                  | Dependencies                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/resource-manager/organizations/{organization_id}/conformance-packs                         | rms:organizationConformancePacks:create | <ul style="list-style-type: none"> <li>organizations:organizations:get</li> <li>organizations:accounts:list</li> <li>organizations:delegatedAdministrators:list</li> <li>organizations:trustedServices:enable</li> <li>organizations:trustedServices:list</li> </ul> |
| DELETE /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id} | rms:organizationConformancePacks:delete | organizations:organizations:get                                                                                                                                                                                                                                      |

| API                                                                                              | Action                                  | Dependencies                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PUT /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id} | rms:organizationConformancePacks:update | <ul style="list-style-type: none"> <li>organizations:organizations:get</li> <li>organizations:accounts:list</li> <li>organizations:delegatedAdministrators:list</li> <li>organizations:trustedServices:enable</li> <li>organizations:trustedServices:list</li> </ul> |
| GET /v1/resource-manager/organizations/{organization_id}/conformance-packs                       | rms:organizationConformancePacks:list   | organizations:organizations:get                                                                                                                                                                                                                                      |
| GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id} | rms:organizationConformancePacks:get    | organizations:organizations:get                                                                                                                                                                                                                                      |
| GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/statuses              | rms:organizationConformancePacks:list   | organizations:organizations:get                                                                                                                                                                                                                                      |
| GET /v1/resource-manager/organizations/{organization_id}/conformance-packs/detailed-statuses     | rms:organizationConformancePacks:get    | organizations:organizations:get                                                                                                                                                                                                                                      |
| POST /v1/resource-manager/domains/{domain_id}/conformance-packs                                  | rms:conformancePacks:create             | <ul style="list-style-type: none"> <li>rf:stack:createStack</li> <li>rf:stack:getStackMetadata</li> <li>rf:stack:listStackResources</li> </ul>                                                                                                                       |

| API                                                                                                     | Action                      | Dependencies                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| DELETE /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}                 | rms:conformancePacks:delete | <ul style="list-style-type: none"> <li>rf:stack:deleteStack</li> <li>rf:stack:getStackMetadata</li> </ul>                                      |
| PUT /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}                    | rms:conformancePacks:update | <ul style="list-style-type: none"> <li>rf:stack:deployStack</li> <li>rf:stack:getStackMetadata</li> <li>rf:stack:listStackResources</li> </ul> |
| GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}                    | rms:conformancePacks:get    | -                                                                                                                                              |
| GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}/compliance         | rms:conformancePacks:get    | -                                                                                                                                              |
| GET /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}/compliance/details | rms:conformancePacks:get    | -                                                                                                                                              |
| GET /v1/resource-manager/domains/{domain_id}/conformance-packs                                          | rms:conformancePacks:list   | -                                                                                                                                              |
| GET /v1/resource-manager/domains/{domain_id}/conformance-packs/compliance/summary                       | rms:conformancePacks:list   | -                                                                                                                                              |

| API                                                                                       | Action                       | Dependencies |
|-------------------------------------------------------------------------------------------|------------------------------|--------------|
| GET /v1/resource-manager/domains/{domain_id}/conformance-packs/scores                     | rms:conformancePacks:list    | -            |
| POST /v1/resource-manager/domains/{domain_id}/stored-queries                              | rms:storedQueries:create     | -            |
| PUT /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}                    | rms:storedQueries:update     | -            |
| DELETE /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}                 | rms:storedQueries:delete     | -            |
| GET /v1/resource-manager/domains/{domain_id}/stored-queries/{query_id}                    | rms:storedQueries:get        | -            |
| GET /v1/resource-manager/domains/{domain_id}/stored-queries                               | rms:storedQueries:list       | -            |
| PUT /v1/resource-manager/domains/{domain_id}/policy-assignments                           | rms:policyAssignments:create | -            |
| DELETE /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id} | rms:policyAssignments:delete | -            |
| GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}    | rms:policyAssignments:get    | -            |



| API                                                                                                             | Action                                 | Dependencies                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1/resource-manager/domains/{domain_id}/policy-assignments                                                 | rms:policyAssignments:get              | -                                                                                                                                                                                                                                                                              |
| PUT /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}                          | rms:policyAssignments:update           | -                                                                                                                                                                                                                                                                              |
| POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/disable                 | rms:policyAssignments:update           | -                                                                                                                                                                                                                                                                              |
| POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/enable                  | rms:policyAssignments:update           | -                                                                                                                                                                                                                                                                              |
| PUT /v1/resource-manager/organizations/{organization_id}/policy-assignments                                     | rms:organizationPolicyAssignments:put  | <ul style="list-style-type: none"> <li>• organizations:organizations:get</li> <li>• organizations:accounts:list</li> <li>• organizations:delegatedAdministrators:list</li> <li>• organizations:trustedServices:enable</li> <li>• organizations:trustedServices:list</li> </ul> |
| GET /v1/resource-manager/organizations/{organization_id}/policy-assignments                                     | rms:organizationPolicyAssignments:list | organizations:organizations:get                                                                                                                                                                                                                                                |
| GET /v1/resource-manager/organizations/{organization_id}/policy-assignments/{organization_policy_assignment_id} | rms:organizationPolicyAssignments:get  | organizations:organizations:get                                                                                                                                                                                                                                                |

| API                                                                                                                  | Action                                   | Dependencies                    |
|----------------------------------------------------------------------------------------------------------------------|------------------------------------------|---------------------------------|
| GET /v1/resource-manager/organizations/{organization_id}/policy-assignment-statuses                                  | rms:organizationPolicyAssignments:list   | organizations:organizations:get |
| GET /v1/resource-manager/organizations/{organization_id}/policy-assignment-detailed-status                           | rms:organizationPolicyAssignments:list   | organizations:organizations:get |
| DELETE /v1/resource-manager/organizations/{organization_id}/policy-assignments/{organization_policy_assignment_id}   | rms:organizationPolicyAssignments:delete | organizations:organizations:get |
| GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states                 | rms:policyStates:get                     | -                               |
| GET /v1/resource-manager/domains/{domain_id}/policy-states                                                           | rms:policyStates:get                     | -                               |
| GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/policy-states                                   | rms:policyStates:get                     | -                               |
| POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states/run-evaluation | rms:policyStates:runEvaluation           | -                               |

| API                                                                                                                   | Action                  | Dependencies                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/policy-states/evaluation-state | rms:policyStates:get    | -                                                                                                                                                                                                                                                                              |
| PUT /v1/resource-manager/domains/{domain_id}/policy-states                                                            | rms:policyStates:update | -                                                                                                                                                                                                                                                                              |
| PUT /v1/resource-manager/domains/{domain_id}/aggregators                                                              | rms:aggregators:create  | <ul style="list-style-type: none"> <li>• organizations:organizations:get</li> <li>• organizations:accounts:list</li> <li>• organizations:delegatedAdministrators:list</li> <li>• organizations:trustedServices:enable</li> <li>• organizations:trustedServices:list</li> </ul> |
| PUT /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}                                              | rms:aggregators:update  | <ul style="list-style-type: none"> <li>• organizations:organizations:get</li> <li>• organizations:accounts:list</li> <li>• organizations:delegatedAdministrators:list</li> <li>• organizations:trustedServices:enable</li> <li>• organizations:trustedServices:list</li> </ul> |
| DELETE /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}                                           | rms:aggregators:delete  | -                                                                                                                                                                                                                                                                              |
| GET /v1/resource-manager/domains/{domain_id}/aggregators                                                              | rms:aggregators:list    | -                                                                                                                                                                                                                                                                              |

| API                                                                                                       | Action                       | Dependencies                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}                                  | rms:aggregators:get          | -                                                                                                                                                                                 |
| GET /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}/aggregator-sources-status        | rms:aggregators:get          | -                                                                                                                                                                                 |
| POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-summary | rms:aggregatorResources:list | <ul style="list-style-type: none"> <li>organizations:organizations:get</li> <li>organizations:delegatedAdministrators:list</li> <li>organizations:trustedServices:list</li> </ul> |
| POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignments/compliance    | rms:aggregatorResources:list | <ul style="list-style-type: none"> <li>organizations:organizations:get</li> <li>organizations:delegatedAdministrators:list</li> <li>organizations:trustedServices:list</li> </ul> |
| POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-details | rms:aggregatorResources:list | <ul style="list-style-type: none"> <li>organizations:organizations:get</li> <li>organizations:delegatedAdministrators:list</li> <li>organizations:trustedServices:list</li> </ul> |
| POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignment/detail         | rms:aggregatorResources:list | <ul style="list-style-type: none"> <li>organizations:organizations:get</li> <li>organizations:delegatedAdministrators:list</li> <li>organizations:trustedServices:list</li> </ul> |

| API                                                                                                           | Action                               | Dependencies                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-resource-config                           | rms:aggregatorResources:get          | -                                                                                                                                                                                       |
| POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/aggregate-discovered-resources       | rms:aggregatorResources:list         | <ul style="list-style-type: none"> <li>• organizations:organizations:get</li> <li>• organizations:delegatedAdministrators:list</li> <li>• organizations:trustedServices:list</li> </ul> |
| POST /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}/run-query                           | rms:aggregatorResources:runQuery     | -                                                                                                                                                                                       |
| POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/aggregate-discovered-resource-counts | rms:aggregatorResources:list         | <ul style="list-style-type: none"> <li>• organizations:organizations:get</li> <li>• organizations:delegatedAdministrators:list</li> <li>• organizations:trustedServices:list</li> </ul> |
| GET /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization                            | rms:aggregationAuthorizations:list   | -                                                                                                                                                                                       |
| PUT /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization                            | rms:aggregationAuthorizations:create | -                                                                                                                                                                                       |

| API                                                                                                            | Action                               | Dependencies |
|----------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| DELETE /v1/resource-manager/domains/{domain_id}/aggregators/aggregation-authorization/{authorized_account_id}  | rms:aggregationAuthorizations:delete | -            |
| DELETE /v1/resource-manager/domains/{domain_id}/aggregators/pending-aggregation-request/{requester_account_id} | rms:aggregationRequests:delete       | -            |
| GET /v1/resource-manager/domains/{domain_id}/aggregators/pending-aggregation-request                           | rms:aggregationRequests:list         | -            |
| PUT /v1/resource-manager/domains/{domain_id}/tracker-config                                                    | rms:trackerConfig:put                | -            |
| DELETE /v1/resource-manager/domains/{domain_id}/tracker-config                                                 | rms:trackerConfig:delete             | -            |
| GET /v1/resource-manager/domains/{domain_id}/tracker-config                                                    | rms:trackerConfig:get                | -            |
| GET /v1/resource-manager/domains/{domain_id}/schemas                                                           | rms:schemas:list                     | -            |
| GET /v1/resource-manager/policy-definitions                                                                    | rms:policyDefinitions:get            | -            |

| API                                                                                                  | Action                    | Dependencies |
|------------------------------------------------------------------------------------------------------|---------------------------|--------------|
| GET /v1/resource-manager/policy-definitions/{policy_definition_id}                                   | rms:policyDefinitions:get | -            |
| GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/history                         | rms:resources:getHistory  | -            |
| GET /v1/resource-manager/domains/{domain_id}/all-resources/{resource_id}/relations                   | rms:resources:getRelation | -            |
| GET /v1/resource-manager/domains/{domain_id}/provider/{provider}/type/{type}/resources/{resource_id} | rms:resources:get         | -            |
| GET /v1/resource-manager/domains/{domain_id}/all-resources                                           | rms:resources:list        | -            |
| GET /v1/resource-manager/domains/{domain_id}/provider/{provider}/type/{type}/resources               | rms:resources:list        | -            |
| POST /v1/resource-manager/domains/{domain_id}/run-query                                              | rms:resources:runQuery    | -            |
| GET /v1/resource-manager/domains/{domain_id}/all-resources/summary                                   | rms:resources:list        | -            |

| API                                                                            | Action                   | Dependencies |
|--------------------------------------------------------------------------------|--------------------------|--------------|
| GET /v1/resource-manager/domains/{domain_id}/all-resources/tags                | rms:resources:list       | -            |
| GET /v1/resource-manager/domains/{domain_id}/all-resources/count               | rms:resources:list       | -            |
| GET /v1/resource-manager/domains/{domain_id}/all-resources/{resource_id}       | rms:resources:get        | -            |
| GET /v1/resource-manager/domains/{domain_id}/resources/{resource_id}/relations | rms:resources:summarize  | -            |
| POST /v1/resource-manager/{resource_type}/{resource_id}/tags/create            | rms::tagResource         | -            |
| POST /v1/resource-manager/{resource_type}/{resource_id}/tags/delete            | rms::unTagResource       | -            |
| GET /v1/resource-manager/{resource_type}/{resource_id}/tags                    | rms::listTagsForResource | -            |
| GET /v1/resource-manager/{resource_type}/tags                                  | rms::listTags            | -            |
| POST /v1/resource-manager/{resource_type}/resource-instances/count             | rms::listResourcesByTag  | -            |



| API                                                                                                                   | Action                                                            | Dependencies                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v1/resource-manager/{resource_type}/resource-instances/filter                                                   | rms::listResourcesByTag                                           | -                                                                                                                                                                                                                                                                                             |
| PUT /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration      | rms:policyAssignmentsRemediation:putRemediationConfiguration      | <ul style="list-style-type: none"> <li>iam:agencies:pass</li> <li>iam:agencies:createServiceLinkedAgencyV5</li> </ul>                                                                                                                                                                         |
| DELETE /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration   | rms:policyAssignmentsRemediation:deleteRemediationConfiguration   | -                                                                                                                                                                                                                                                                                             |
| GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-configuration      | rms:policyAssignmentsRemediation:getRemediationConfiguration      | -                                                                                                                                                                                                                                                                                             |
| POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution         | rms:policyAssignmentsRemediation:runRemediation                   | <ul style="list-style-type: none"> <li>functiongraph:function:invokeAsync</li> <li>functiongraph:function:getFunctionConfig</li> <li>rf:stack:create</li> <li>rf:stack:delete</li> <li>rf:stack:getTemplate</li> <li>rf:stack:getMetadata</li> <li>rf:privateTemplate:showMetadata</li> </ul> |
| GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution-statuses | rms:policyAssignmentsRemediation:listRemediationExecutionStatuses | -                                                                                                                                                                                                                                                                                             |

| API                                                                                                                            | Action                                                            | Dependencies |
|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|--------------|
| POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution-statuses/summary | rms:policyAssignmentsRemediation:listRemediationExecutionStatuses | -            |
| POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception/create           | rms:policyAssignmentsRemediation:createRemediationExceptions      | -            |
| POST /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception/delete           | rms:policyAssignmentsRemediation:deleteRemediationExceptions      | -            |
| GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-exception                   | rms:policyAssignmentsRemediation:listRemediationExceptions        | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-256](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for Config.

**Table 3-256** Resource types supported by Config

| Resource Type                 | URN                                                                                                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------|
| policyAssignments             | rms::<account-id>:policyAssignments:<policy-assignment-id>                                             |
| aggregationAuthorizations     | rms::<account-id>:aggregationAuthorizations:<authorized-account-id>                                    |
| policyAssignmentsRemediation  | rms::<account-id>:policyAssignmentsRemediation:<policy-assignment-id>                                  |
| aggregators                   | rms::<account-id>:aggregators:<aggregator-id>                                                          |
| organizationConformancePacks  | rms::<account-id>:organizationConformancePacks:<organization-id>/<organization-conformance-pack-id>    |
| conformancePacks              | rms::<account-id>:conformancePacks:<conformance-pack-id>                                               |
| storedQueries                 | rms::<account-id>:storedQueries:<query-id>                                                             |
| organizationPolicyAssignments | rms::<account-id>:organizationPolicyAssignments:<organization-id>/<organization-policy-assignments-id> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, config) apply only to operations of the xx service. For details, see [Table 3-257](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.

- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by Config

The following table lists the condition keys that you can define in identity policies for Config. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-257** Service-specific condition keys supported by Config

| Service-specific Condition Key               | Type   | Single-valued/<br>Multivalued | Description                                                                                            |
|----------------------------------------------|--------|-------------------------------|--------------------------------------------------------------------------------------------------------|
| <a href="#">rms:AuthorizedAccountOrgPath</a> | string | Single-valued                 | Filters access based on the Organizations Path of the specified resource aggregate authorized account. |
| <a href="#">rms:TrackerBucketName</a>        | string | Single-valued                 | Filters access based on the specified dump target bucket name.                                         |
| <a href="#">rms:TrackerBucketPathPrefix</a>  | string | Single-valued                 | Filters access based on the specified dump target bucket prefix.                                       |

### Examples of Condition Keys

- `rms:AuthorizedAccountOrgPath`

For example, preventing aggregation authorization to accounts outside the current organization.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:aggregationAuthorizations:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:AuthorizedAccountOrgPath": [
            "organization_id/root_id/ou_id" [Note: Enter organization path ID.]
          ]
        }
      }
    }
  ]
}
```

- rms:TrackerBucketName

For example, trackerConfig is not allowed to deliver data to unexpected OBS buckets.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketName": [
            "BucketName"
          ]
        }
      }
    }
  ]
}
```

- rms:TrackerBucketPathPrefix

For example, trackerConfig is not allowed to deliver data to unexpected OBS Path.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketPathPrefix": [
            "BucketFolder"
          ]
        }
      }
    }
  ]
}
```

### 3.14.6 Tag Management Service (TMS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are

available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by TMS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by TMS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for TMS.

**Table 3-258** Actions supported by TMS

| Action                   | Description                                  | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------|----------------------------------------------|--------------|-----------------------------|---------------|-------|
| tms:predefineTags:create | Grants permission to create predefined tags. | Write        | -                           | -             | -     |
| tms:predefineTags:update | Grants permission to update predefined tags. | Write        | -                           | -             | -     |
| tms:predefineTags:delete | Grants permission to delete predefined tags. | Write        | -                           | -             | -     |

Each API of TMS usually supports one or more actions. [Table 3-259](#) lists the supported actions and dependencies.

**Table 3-259** Actions and dependencies supported by TMS APIs

| API                                 | Action                   | Dependencies |
|-------------------------------------|--------------------------|--------------|
| POST /v1.0/predefine_tags/action    | tms:predefineTags:create | -            |
| PUT /v1.0/predefine_tags            | tms:predefineTags:update | -            |
| POST 01 /v1.0/predefine_tags/action | tms:predefineTags:delete | -            |

## Resources

TMS does not support resource-level authorization. To allow access to TMS, use a wildcard (\*) in the Resource element of the identity policy, indicating that the identity policy will be applied to all resources.

## Conditions

TMS does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.14.7 Enterprise Project Management Service (EPS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#).

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by EPS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.



- If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
- If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
- If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by EPS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for EPS.

**Table 3-260** Actions supported by EPS

| Action                         | Description                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| eps:enterpriseProjects:list    | Grants permission to view the enterprise project list. | List         | enterpriseProject*          | -             | -     |
| eps:enterpriseProjects:create  | Grants permission to create an enterprise project.     | Write        | enterpriseProject*          | -             | -     |
| eps:enterpriseProjects:update  | Grants permission to modify an enterprise project.     | Write        | enterpriseProject*          | -             | -     |
| eps:enterpriseProjects:enable  | Grants permission to enable an enterprise project.     | Write        | enterpriseProject*          | -             | -     |
| eps:enterpriseProjects:disable | Grants permission to disable an enterprise project.    | Write        | enterpriseProject*          | -             | -     |

| Action                        | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| eps:enterpriseProjects:delete | Grants permission to delete an enterprise project.            | Write        | enterpriseProject*          | -             | -     |
| eps:resources:list            | Grants permission to view resources in an enterprise project. | List         | enterpriseProject*          | -             | -     |
| eps:resources:add             | Grants permission to add resources to an enterprise project.  | Write        | enterpriseProject*          | -             | -     |

Each API of EPS usually supports one or more actions. [Table 3-261](#) lists the supported actions and dependencies.

**Table 3-261** Actions and dependencies supported by EPS APIs

| API                                                           | Action                        | Dependencies |
|---------------------------------------------------------------|-------------------------------|--------------|
| GET /v1.0/enterprise-projects                                 | eps:enterpriseProjects:list   | -            |
| POST /v1.0/enterprise-projects                                | eps:enterpriseProjects:create | -            |
| PUT /v1.0/enterprise-projects/{enterprise_project_id}         | eps:enterpriseProjects:update | -            |
| POST /v1.0/enterprise-projects/{enterprise_project_id}/action | eps:enterpriseProjects:enable | -            |

| API                                                                      | Action                         | Dependencies         |
|--------------------------------------------------------------------------|--------------------------------|----------------------|
| POST /v1.0/enterprise-projects/{enterprise_project_id}/action            | eps:enterpriseProjects:disable | -                    |
| DELETE /v1.0/enterprise-projects/{enterprise_project_id}                 | eps:enterpriseProjects:delete  | -                    |
| POST /v1.0/enterprise-projects/{enterprise_project_id}/resources/filter  | eps:resources:list             | -                    |
| POST /v1.0/enterprise-projects/{enterprise_project_id}/resources-migrate | eps:resources:add              | eps:resources:remove |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-262](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for EPS.

**Table 3-262** Resource types supported by EPS

| Resource Type     | URN                                                         |
|-------------------|-------------------------------------------------------------|
| enterpriseProject | eps::<account-id>:enterpriseProject:<enterprise-project-id> |

## Conditions

EPS does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.14.8 Cloud Eye

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by Cloud Eye, see [Resources](#).

- **Condition Key** contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.

- If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Cloud Eye, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for identity policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Cloud Eye.

**Table 3-263** Actions supported by Cloud Eye

| Action                | Description                                           | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                   | Alias                  |
|-----------------------|-------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| ces:alarms:create     | Grants permission to create an alarm rule.            | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">ces:namespace</a></li> </ul> | -                      |
| ces:alarms:list       | Grants permission to list alarm rules.                | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                           | -                      |
| ces:alarms:put        | Grants permission to update an alarm rule.            | Write        | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                              | • ces:alarms:onoff:put |
|                       |                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>                                                                                           |                        |
| ces:alarms:put Action | Grants permission to enable or disable an alarm rule. | Write        | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                              | • ces:alarms:put       |

| Action                        | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                  | Alias                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| ces:alarms:get                | Grants permission to query an alarm rule.                                           | Read         | alarm *                     | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | <ul style="list-style-type: none"> <li>ces:alarms:list</li> </ul>             |
| ces:alarms:delete             | Grants permission to delete an alarm rule.                                          | Write        | alarm *                     | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | -                                                                             |
| ces:alarms:getInstanceStatus  | Grants permission to query the instance alarm status.                               | Read         | alarm *                     | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | <ul style="list-style-type: none"> <li>ces:alarmInstanceStatus:get</li> </ul> |
| ces:alarms:getClassInfo       | Grants permission to query the number of alarm rules of different types.            | Read         | alarm *                     | <ul style="list-style-type: none"> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>ces:alarmClassInfo:get</li> </ul>      |
| ces:alarms:listNamespaces     | Grants permission to list alarm namespaces.                                         | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | <ul style="list-style-type: none"> <li>ces:alarmNamespaces:list</li> </ul>    |
| ces:alarms:listOneClickAlarms | Grants permission to list services and resources that support one-click monitoring. | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | <ul style="list-style-type: none"> <li>ces:oneClickAlarms:list</li> </ul>     |
| ces:alarms:putOneClickAlarms  | Grants permission to batch enable or disable one-click monitoring.                  | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                          | <ul style="list-style-type: none"> <li>ces:oneClickAlarms:put</li> </ul>      |

| Action                           | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                      | Alias                                                               |
|----------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| ces:alarms:addResources          | Grants permission to batch add resources to an alarm rule.                   | Write        | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• ces:alarms:put</li> </ul>  |
| ces:alarms:deleteResources       | Grants permission to batch delete resources from an alarm rule.              | Write        | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• ces:alarms:put</li> </ul>  |
| ces:alarms:getPolicies           | Grants permission to query policies in an alarm rule.                        | Read         | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• ces:alarms:get</li> </ul>  |
| ces:alarms:getResources          | Grants permission to list monitored resources in an alarm rule.              | Read         | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• ces:alarms:list</li> </ul> |
| ces:alarms:updatePolicies        | Grants permission to update policies of an alarm rule.                       | Write        | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• ces:alarms:put</li> </ul>  |
| ces:alarms:putAlarmNotifications | Grants permission to modify alarm notification information in an alarm rule. | Write        | alarm *                     | <ul style="list-style-type: none"> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | <ul style="list-style-type: none"> <li>• ces:alarms:put</li> </ul>  |

| Action                                   | Description                                                                                                         | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                          |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------------|
| ces:alarms:putNotificationMaskRules      | Grants permission to configure alarm masking rules.                                                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:notificationMasks:update</li> </ul> |
| ces:alarms:listNotificationMaskResources | Grants permission to list resources for which alarm notifications have been masked.                                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:notificationMasks:list</li> </ul>   |
| ces:alarms:deleteNotificationMaskRules   | Grants permission to batch delete alarm notification masking rules.                                                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:notificationMasks:delete</li> </ul> |
| ces:alarms:listNotificationMaskRules     | Grants permission to list alarm notification masking rules.                                                         | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:notificationMasks:list</li> </ul>   |
| ces:alarms:createOneClickAlarms          | Grants permission to enable one-click monitoring.                                                                   | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:oneClickAlarms:post</li> </ul>      |
| ces:alarms:putOneClickAlarmPolicies      | Grants permission to batch enable or disable alarm policies in alarm rules for a service with one-click monitoring. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:oneClickAlarms:put</li> </ul>       |



| Action                                   | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                                    |
|------------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------------------------------------------------------------------|
| ces:alarms:putOneClickAlarmNotifications | Grants permission to batch modify alarm notification rules of one-click monitoring for a service. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:oneClickAlarms:updateNotifications</li> </ul> |
| ces:alarms:deleteOneClickAlarms          | Grants permission to batch disable one-click monitoring.                                          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:oneClickAlarms:delete</li> </ul>              |
| ces:notificationGroup:delete             | Grants permission to delete a notification group.                                                 | Write        | -                           | -                                     | -                                                                                        |
| ces:notificationGroup:convertObject      | Grants permission to convert a recipient.                                                         | Write        | -                           | -                                     | -                                                                                        |
| ces:notificationGroup:listSubscriptions  | Grants permission to list subscriptions of a notification group.                                  | List         | -                           | -                                     | -                                                                                        |
| ces:widgets:put                          | Grants permission to batch update graphs.                                                         | Write        | -                           | <a href="#">ces:namespace</a>         | -                                                                                        |
| ces:widgets:create                       | Grants permission to create a graph.                                                              | Write        | -                           | <a href="#">ces:namespace</a>         | -                                                                                        |

| Action                   | Description                                             | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|--------------------------|---------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| ces:widgets:delete       | Grants permission to delete a graph.                    | Write        | -                           | -                                     | -     |
| ces:dashboards:create    | Grants permission to create a dashboard.                | Write        | dashboard *                 | -                                     | -     |
|                          |                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| ces:dashboards:get       | Grants permission to query details about a dashboard.   | Read         | dashboard *                 | -                                     | -     |
|                          |                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| ces:dashboards:list      | Grants permission to list dashboards.                   | List         | dashboard *                 | -                                     | -     |
|                          |                                                         |              | -                           | <a href="#">g:EnterpriseProjectId</a> |       |
| ces:dashboards:put       | Grants permission to update a dashboard.                | Write        | dashboard *                 | <a href="#">g:EnterpriseProjectId</a> | -     |
| ces:widgets:list         | Grants permission to query graphs added to a dashboard. | List         | -                           | -                                     | -     |
| ces:dashboards:delete    | Grants permission to batch delete dashboards.           | Write        | dashboard *                 | <a href="#">g:EnterpriseProjectId</a> | -     |
| ces:systemDashboards:get | Grants permission to batch query system dashboards.     | Read         | -                           | -                                     | -     |

| Action                                         | Description                                                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------|
| ces:systemDashboard:put                        | Grants permission to update a system dashboard.                                                            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:systemDashboard:update</li> </ul> |
| ces:widgets:get                                | Grants permission to query a graph.                                                                        | Read         | -                           | -             | -                                                                            |
| ces:dashboard:listServices                     | Grants permission to list cloud service dashboards.                                                        | List         | -                           | -             | -                                                                            |
| ces:dashboard:listResourceStatistics           | Grants permission to query resource statistics of a dimension on a cloud service dashboard.                | List         | -                           | -             | -                                                                            |
| ces:dashboard:listAlarmStatistics              | Grants permission to query alarm statistics by severity on a cloud service dashboard.                      | List         | -                           | -             | -                                                                            |
| ces:dashboard:listResourceGroupAlarmStatistics | Grants permission to query alarm statistics by severity for a resource group on a cloud service dashboard. | List         | -                           | -             | -                                                                            |

| Action                                       | Description                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                           |
|----------------------------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------|
| ces:dashboardGroups:delete                   | Grants permission to delete a graph group.                       | Write        | -                           | -             | -                                                                               |
| ces:dashboardGroups:list                     | Grants permission to view a graph group.                         | List         | -                           | -             | -                                                                               |
| ces:dashboardGroups:create                   | Grants permission to create a graph group.                       | Write        | -                           | -             | -                                                                               |
| ces:dashboardGroups:update                   | Grants permission to batch update graph groups.                  | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:dashboardGroups:put</li> </ul>       |
| ces:metrics:list                             | Grants permission to list metrics.                               | List         | -                           | -             | -                                                                               |
| ces:metricData:create                        | Grants permission to report metrics.                             | Write        | -                           | -             | -                                                                               |
| ces:metricData:get                           | Grants permission to query data of a metric.                     | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:metricData:list</li> </ul>           |
| ces:metricData:list                          | Grants permission to batch query metric data.                    | List         | -                           | -             | -                                                                               |
| ces:namespacesDimensions:listAgentDimensions | Grants permission to query Agent-related metrics of an instance. | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:namespacesDimensions:list</li> </ul> |

| Action                        | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------------------------|
| ces:namespacesDimensions:list | Grants permission to batch query metric dimensions.                               | List         | -                           | ces:namespace | -                                                                                                   |
| ces:namespacesDimensions:get  | Grants permission to batch query the dimension hierarchy of specified namespaces. | Read         | -                           | ces:namespace | <ul style="list-style-type: none"> <li>ces:namespacesDimensions:list</li> </ul>                     |
| ces:agent:putHeartBeat        | Grants permission to update the heartbeat status of a server.                     | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:heartbeat:post</li> </ul>                                |
| ces:agent:putStatus           | Grants permission to update the Agent status of an instance.                      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:heartbeat:post</li> </ul>                                |
| ces:agent:getStatus           | Grants permission to query the Agent status of an instance.                       | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentStatus:get</li> </ul>                               |
| ces:agent:listStatuses        | Grants permission to batch query the Agent status of instances.                   | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentStatus:get</li> <li>ces:agentStatus:list</li> </ul> |

| Action                                | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                    |
|---------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------------------------------------------------------------|
| ces:agent:putVersion                  | Grants permission to update the Agent version of an instance. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentUpgrade:post</li> </ul>                  |
| ces:metrics:listSupported             | Grants permission to batch query all supported metrics.       | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:currentRegionSupportedMetrics:list</li> </ul> |
| ces:namespaceMetrics:list             | Grants permission to batch query metrics.                     | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:currentRegionSupportedMetrics:list</li> </ul> |
| ces:ecsInstanceStatistics:get         | Grants permission to batch query ECS CPU metric statistics.   | Read         | -                           | -             | -                                                                                        |
| ces:evsInstanceStatistics:get         | Grants permission to batch query EVS metric statistics.       | Read         | -                           | -             | -                                                                                        |
| ces:namespaceDimensions:listInstances | Grants permission to batch query instances in a dimension.    | List         | -                           | ces:namespace | <ul style="list-style-type: none"> <li>ces:namespaceDimensions:list</li> </ul>           |
| ces:metaData:get                      | Grants permission to batch query metadata of dimensions.      | Read         | -                           | ces:namespace | <ul style="list-style-type: none"> <li>ces:metaData:list</li> </ul>                      |
| ces:resourcesMetadata:list            | Grants permission to batch query metadata of resources.       | List         | -                           | ces:namespace | -                                                                                        |

| Action                         | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                    |
|--------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------------------------------|
| ces:metrics:listStatistics     | Grants permission to batch query dimensional metric statistics.            | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:metrics:list</li> </ul>       |
| ces:agent:listPrefixMetrics    | Grants permission to batch query metrics with prefixes.                    | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:prefixMetrics:list</li> </ul> |
| ces:metricData:export          | Grants permission to create a metric report.                               | Write        | -                           | -             | -                                                                        |
| ces:sortedMetrics:list         | Grants permission to batch query the metric order of specified dimensions. | List         | -                           | -             | -                                                                        |
| ces:sortedMetrics:create       | Grants permission to sort metrics for a specified dimension.               | Write        | -                           | -             | -                                                                        |
| ces:namespaces:list            | Grants permission to batch query namespaces.                               | List         | -                           | -             | -                                                                        |
| ces:vpclInstanceStatistics:get | Grants permission to query VPC metric statistics.                          | Read         | -                           | -             | -                                                                        |

| Action                           | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                          |
|----------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------------------------------------|
| ces:resourcesConsole:list        | Grants permission to batch query resource data of a namespace on the console. | List         | -                           | ces:namespace | -                                                                              |
| ces:metricData:listPercentile    | Grants permission to batch query metric percentages.                          | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:percentageMetricData:get</li> </ul> |
| ces:metrics:listKeyMetrics       | Grants permission to query key metrics.                                       | List         | -                           | ces:namespace | -                                                                              |
| ces:alarmHistoryReportJob:create | Grants permission to batch create tasks for alarm record reporting.           | Write        | -                           | -             | -                                                                              |
| ces:alarmHistoryReportJob:list   | Grants permission to batch query tasks for alarm record reporting.            | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:metricReportJobs:list</li> </ul>    |
| ces:alarmHistoryReportJob:delete | Grants permission to batch delete tasks for alarm record reporting.           | Write        | -                           | -             | -                                                                              |



| Action                               | Description                                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                          |
|--------------------------------------|-------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------|
| ces:alarmHistoriesReportJob:download | Grants permission to batch query resource data of a namespace on the console. | Read         | -                           | -             | -                                                              |
| ces:metricReportJob:download         | Grants permission to download a metric report.                                | Read         | -                           | -             | -                                                              |
| ces:metricReportJobs:list            | Grants permission to batch query metric reporting tasks.                      | List         | -                           | -             | -                                                              |
| ces:metricReportJob:create           | Grants permission to batch create metric reporting tasks.                     | Write        | -                           | -             | -                                                              |
| ces:metricReportJobs:delete          | Grants permission to batch delete metric reporting tasks.                     | Write        | -                           | -             | -                                                              |
| ces:quotas:get                       | Grants permission to query quotas.                                            | Read         | -                           | -             | -                                                              |
| ces:i18n:list                        | Grants permission to obtain internationalization information.                 | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:i18n:get</li> </ul> |

| Action                          | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------------------------------------------------|
| ces:resourcesStatistics:list    | Grants permission to batch query resource statistics.                             | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:resourcesStatistics:get</li> </ul> |
| ces:supportedFeature:list       | Grants permission to batch query supported features.                              | List         | -                           | -             | -                                                                             |
| ces:asyncTasks:list             | Grants permission to batch query asynchronous tasks.                              | List         | -                           | -             | -                                                                             |
| ces:agent:getAgencySecurityInfo | Grants permission to query security information of an agency.                     | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agency:get</li> </ul>              |
| ces:agent:putConfigStatus       | Grants permission to update the configuration status of a server monitoring rule. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentConfigStatus:put</li> </ul>   |
| ces:agent:getConfigStatus       | Grants permission to query the configuration status of a server.                  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentConfigStatus:get</li> </ul>   |
| ces:agent:listExtensionStatuses | Grants permission to batch query the extension status of specified servers.       | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentStatus:get</li> </ul>         |

| Action                      | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                                |
|-----------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------------------------------------------------|
| ces:agent:put               | Grants permission to update the server monitoring metrics of a server.         | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentClientMonitor:put</li> </ul>                                         |
| ces:agent:createProf        | Grants permission to create a profile for a server.                            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentClientProfile:post</li> </ul>                                        |
| ces:agent:listProcesses     | Grants permission to query the monitored process data of a server.             | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentProcessesMetricData:list</li> <li>ces:agentProcesses:list</li> </ul> |
| ces:agent:listPlugins       | Grants permission to batch query the plug-in information of specified servers. | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentClientPluginInfo:get</li> </ul>                                      |
| ces:agent:putPlugins        | Grants permission to batch update the plug-in information of a server.         | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentClientPluginInfo:put</li> </ul>                                      |
| ces:agent:putProcessActions | Grants permission to batch update process actions of a server.                 | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentProcesses:put</li> </ul>                                             |

| Action                           | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------------------|
| ces:agentProcesses:list          | Grants permission to batch query process details of a server.               | List         | -                           | -             | -                                                                                       |
| ces:agent:putProcesses           | Grants permission to batch update process details of a server.              | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentProcesses:create</li> </ul>             |
| ces:agent:createSpecifiedProcess | Grants permission to batch create process records of specified servers.     | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:instanceSpecifiedProcesses:create</li> </ul> |
| ces:agent:listSpecifiedProcesses | Grants permission to batch query specified processes on a server.           | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:instanceSpecifiedProcesses:list</li> </ul>   |
| ces:agent:deleteSpecifiedProcess | Grants permission to batch delete specified processes on specified servers. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:instanceSpecifiedProcesses:delete</li> </ul> |
| ces:agent:listTaskInvoke         | Grants permission to batch query tasks called by a server.                  | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentTask:get</li> </ul>                     |

| Action                           | Description                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                 |
|----------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------------|
| ces:agent:submitTaskResult       | Grants permission to report task results of a server.               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentTask:post</li> </ul>                  |
| ces:agent:listTelescopeConfigs   | Grants permission to batch query nested configurations of a server. | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentClientTelescopeConfigs:get</li> </ul> |
| ces:agent:listConfChecks         | Grants permission to batch query DNS records of a server.           | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:confChecks:get</li> </ul>                  |
| ces:agent:listTaskInvocations    | Grants permission to batch query Agent tasks of a server.           | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:taskInvocation:get</li> </ul>              |
| ces:agent:createAgentInvocations | Grants permission to batch create Agent tasks.                      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:taskInvocation:post</li> </ul>             |
| ces:agent:listAgentInstallSteps  | Grants permission to query the Agent installation step details.     | List         | -                           | -             | -                                                                                     |
| ces:agent:listMetricData         | Grants permission to batch query Agent-related metric details.      | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentmetricdata:list</li> </ul>            |
| ces:agent:listInstancesWithAgent | Grants permission to query Agent information of a server.           | List         | -                           | -             | -                                                                                     |

| Action                                | Description                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                 |
|---------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------------|
| ces:agent:updateAgentAvailabilityTask | Grants permission to update an Agent availability task.                   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentClientAvailabilityTask:put</li> </ul> |
| ces:agent:getAgentAvailabilityTask    | Grants permission to get Agent availability task details.                 | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:agentClientAvailabilityTask:get</li> </ul> |
| ces:availabilityMonitorTask:create    | Grants permission to batch create availability monitoring tasks.          | Write        | -                           | -             | -                                                                                     |
| ces:availabilityMonitorTask:list      | Grants permission to list availability monitoring tasks.                  | List         | -                           | -             | -                                                                                     |
| ces:availabilityMonitorTask:get       | Grants permission to query details about an availability monitoring task. | Read         | -                           | -             | -                                                                                     |
| ces:availabilityMonitorTask:update    | Grants permission to modify an availability monitoring task.              | Write        | -                           | -             | -                                                                                     |
| ces:availabilityMonitorTask:delete    | Grants permission to delete an availability monitoring task.              | Write        | -                           | -             | -                                                                                     |

| Action                          | Description                                            | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|---------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| ces:obsTransfers:create         | Grants permission to configure an OBS dump rule.       | Write        | -                           | -                                     | -                                                                                 |
| ces:obsTransfers:listBuckets    | Grants permission to list OBS buckets.                 | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>ces:obsBuckets:list</li> </ul>             |
| ces:obsTransfers:put            | Grants permission to modify a transfer object.         | Write        | -                           | -                                     | -                                                                                 |
| ces:obsTransfers:get            | Grants permission to query a transfer object.          | Read         | -                           | -                                     | -                                                                                 |
| ces:obsTransfers:list           | Grants permission to batch query OBS dump information. | List         | -                           | -                                     | -                                                                                 |
| ces:alarmHistory:list           | Grants permission to list historical alarms.           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:alarmHistory:listNamespaces | Grants permission to list namespaces of alarm records. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:alarmHistoryNamespaces:list</li> </ul> |
| ces:alarmHistory:statistics     | Grants permission to query alarm statistics.           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:alarmsStatistics:get</li> </ul>        |

| Action                                        | Description                                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                           |
|-----------------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|---------------------------------------------------------------------------------|
| ces:customAlarmTemplates:create               | Grants permission to create a custom alarm template.                           | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                               |
| ces:customAlarmTemplates:delete               | Grants permission to delete a custom alarm template.                           | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                               |
| ces:customAlarmTemplates:get                  | Grants permission to query a custom alarm template.                            | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:customAlarmTemplates:list</li> </ul> |
| ces:customAlarmTemplates:list                 | Grants permission to list custom alarm templates.                              | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                               |
| ces:customAlarmTemplates:listAssociatedAlarms | Grants permission to list alarm rules associated with a custom alarm template. | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                               |
| ces:customAlarmTemplates:put                  | Grants permission to update a custom alarm template.                           | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                               |



| Action                                             | Description                                                                                                           | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| ces:customAlarmTemplates:associateResourceGroup    | Grants permission to modify the configurations for asynchronously associating an alarm template with resource groups. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:customAlarmTemplates:put</li> </ul>    |
| ces:customAlarmTemplates:disassociateResourceGroup | Grants permission to disassociate an alarm template from resource groups.                                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:customAlarmTemplates:create</li> </ul> |
| ces:alarmsContacts:list                            | Grants permission to list contacts.                                                                                   | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:alarmsContacts:get                             | Grants permission to query a contact.                                                                                 | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:notificationGroup:create                       | Grants permission to create a notification group.                                                                     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:notificationObject:list                        | Grants permission to list recipients.                                                                                 | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:notificationObject:create                      | Grants permission to create a recipient.                                                                              | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:notificationObject:delete                      | Grants permission to batch delete recipients.                                                                         | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |

| Action                                      | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                             |
|---------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------------------------|
| ces::listNotificationSubscriptions          | Grants permission to list notification subscriptions.                           | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:alarms:listNotificationSubscriptions</li> </ul>        |
| ces::batchCreateNotificationSubscriptions   | Grants permission to batch create notification subscriptions.                   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:alarms:batchCreateNotificationSubscriptions</li> </ul> |
| ces:alarms:listNotificationTemplates        | Grants permission to list custom notification templates.                        | List         | -                           | -             | -                                                                                                 |
| ces:alarms:createNotificationTemplate       | Grants permission to add a custom notification template.                        | Write        | -                           | -             | -                                                                                                 |
| ces:alarms:batchDeleteNotificationTemplates | Grants permission to delete a custom notification template.                     | Write        | -                           | -             | -                                                                                                 |
| ces:alarms:updateNotificationTemplate       | Grants permission to modify a custom notification template.                     | Write        | -                           | -             | -                                                                                                 |
| ces:alarms:listPresetNotificationTemplates  | Grants permission to obtain the fields and field locations of preset templates. | List         | -                           | -             | -                                                                                                 |

| Action                                               | Description                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                                  |
|------------------------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------------------------------------------------------------|
| ces:alarms:listNotificationTemplateAssociationAlarms | Grants permission to list alarms associated with a notification template. | List         | -                           | -             | -                                                                                                      |
| ces:events:post                                      | Grants permission to report an event.                                     | Write        | -                           | -             | -                                                                                                      |
| ces:events:get                                       | Grants permission to query details about an event.                        | Read         | -                           | -             | -                                                                                                      |
| ces:events:list                                      | Grants permission to list events.                                         | List         | -                           | -             | -                                                                                                      |
| ces:events:listEventStatistics                       | Grants permission to batch query event statistics.                        | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:eventData:list</li> <li>ces:eventsStatistics:get</li> </ul> |
| ces:events:listSystemEventNames                      | Grants permission to batch query system event data.                       | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:systemEventNames:list</li> </ul>                            |
| ces:events:listCustomEventNames                      | Grants permission to batch query custom event data.                       | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:customEventNames:list</li> </ul>                            |
| ces:events:createSubscription                        | Grants permission to create an event alarm.                               | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:eventSubscription:create</li> </ul>                         |

| Action                         | Description                                                  | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                     |
|--------------------------------|--------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------|
| ces:events:listSystemEvents    | Grants permission to list system events.                     | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:systemEvents:list</li> </ul>   |
| ces:events:listSystemEventMeta | Grants permission to query the system event whitelist.       | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:sysEventsNames:list</li> </ul> |
| ces:eventData:get              | Grants permission to query server configurations.            | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:sapEventData:list</li> </ul>   |
| ces:dataShareJob:list          | Grants permission to list data dump tasks.                   | List         | -                           | -             | -                                                                         |
| ces:dataShareJob:create        | Grants permission to create a data dump task.                | Write        | -                           | -             | -                                                                         |
| ces:dataShareJob:delete        | Grants permission to delete a data dump task.                | Write        | -                           | -             | -                                                                         |
| ces:dataShareJob:get           | Grants permission to query details about a data dump task.   | Read         | -                           | -             | -                                                                         |
| ces:dataShareJob:put           | Grants permission to modify the status for a data dump task. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:dataShareJob:action</li> </ul> |

| Action                                 | Description                                                                               | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                    |
|----------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|--------------------------------------------------------------------------|
| ces:resourceGroups:addResources        | Grants permission to batch add resources to a resource group.                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:resourceGroups:put</li> </ul> |
| ces:resourceGroups:create              | Grants permission to create a resource group.                                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                        |
| ces:resourceGroups:delete              | Grants permission to delete a resource group.                                             | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                        |
| ces:resourceGroups:deleteResources     | Grants permission to batch delete resources from a resource group.                        | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:resourceGroups:put</li> </ul> |
| ces:resourceGroups:get                 | Grants permission to query a resource group.                                              | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                        |
| ces:resourceGroups:getServiceResources | Grants permission to query resources of a dimension and service type in a resource group. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:resourceGroups:get</li> </ul> |

| Action                                         | Description                                                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias                                                                                                              |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| ces:resourceGroups:list                        | Grants permission to list all resource groups.                                                         | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             | <ul style="list-style-type: none"> <li>ces:resourceGroups:get</li> </ul>                                           |
| ces:resourceGroups:put                         | Grants permission to update a resource group.                                                          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             | -                                                                                                                  |
| ces:resourceGroups:putAssociationAlarmTemplate | Grants permission to modify the configurations for associating an alarm template with resource groups. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             | <ul style="list-style-type: none"> <li>ces:resourceGroups:put</li> </ul>                                           |
| ces:resourceGroups:listServices                | Grants permission to batch query service categories of a resource group.                               | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                             | <ul style="list-style-type: none"> <li>ces:resourceGroups:get</li> <li>ces:resourceGroups:services:list</li> </ul> |
| ces:tags:create                                | Grants permission to batch create tags of a type.                                                      | Write        | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>ces:tags:action</li> </ul>                                                  |
| ces:tags:list                                  | Grants permission to list Cloud Eye tags.                                                              | List         | -                           | -                                                                                                                                 | <ul style="list-style-type: none"> <li>ces:projecttags:list</li> </ul>                                             |
| ces:tags:listByResource                        | Grants permission to list resource tags.                                                               | List         | -                           | -                                                                                                                                 | -                                                                                                                  |

| Action                                        | Description                                                            | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias                                                                           |
|-----------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| ces:tags:listResources                        | Grants permission to list resources by tag.                            | List         | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>• ces:resourceinstances: list</li> </ul> |
| ces:agency:get                                | Grants permission to query agencies and roles.                         | Read         | -                           | -                                                                                                                                     | -                                                                               |
| ces:agency:post                               | Grants permission to create agencies and roles.                        | Write        | -                           | -                                                                                                                                     | -                                                                               |
| ces:monitorOverview:listServiceResources      | Grants permission to list resources under a cloud service in Overview. | List         | -                           | <a href="#">ces:namespace</a>                                                                                                         | -                                                                               |
| ces:monitorOverview:updateFavorite            | Grants permission to batch add or remove items from favorites.         | Write        | -                           | -                                                                                                                                     | -                                                                               |
| ces:monitorOverview:listServiceResourceGroups | Grants permission to list resource groups in Overview.                 | List         | -                           | -                                                                                                                                     | -                                                                               |
| ces:monitorOverview:updateKeyMetrics          | Grants permission to batch set key metrics.                            | Write        | -                           | -                                                                                                                                     | -                                                                               |
| ces:monitorOverview:listSiteMonitorStatistics | Grants permission to query website monitoring statistics.              | List         | -                           | -                                                                                                                                     | -                                                                               |

| Action                                | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                                             |
|---------------------------------------|--------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------------------------------|
| ces:siteMonitorRule:list              | Grants permission to batch query website monitors.           | List         | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:remoteChecks:list</li> </ul>           |
| ces:siteMonitorRule:listDetectResults | Grants permission to batch query website monitoring results. | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>ces:siteMonitorDetectResult:get</li> </ul> |
| ces:siteMonitorRule:listSites         | Grants permission to list all website monitors.              | List         | -                           | -                                     | <ul style="list-style-type: none"> <li>ces:remoteCheckSites:list</li> </ul>       |
| ces:siteMonitorRule:delete            | Grants permission to batch delete website monitors.          | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:siteMonitorRule:create            | Grants permission to create a website monitor.               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | <ul style="list-style-type: none"> <li>ces:remoteChecks:create</li> </ul>         |
| ces:siteMonitorRule:put               | Grants permission to update a website monitor.               | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |
| ces:siteMonitorRule:get               | Grants permission to query a website monitoring rule.        | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -                                                                                 |



| Action                                | Description                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                  |
|---------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------------------|
| ces:siteMonitorRule:listDefaultSites  | Grants permission to batch query checkpoints supported by the system. | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:remoteCheckSites:list</li> </ul>            |
| ces:siteMonitorRule:getStatistic      | Grants permission to query website monitoring statistics.             | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:statisticsSiteMonitor:get</li> </ul>        |
| ces:siteMonitorRule:putDataCenter     | Grants permission to update a website monitoring data center.         | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:siteMonitorRuleDataCenter:update</li> </ul> |
| ces:siteMonitorRule:getDataCenter     | Grants permission to query a website monitoring data center.          | Read         | -                           | -             | -                                                                                      |
| ces:siteMonitorRule:showHealthCheck   | Grants permission to query website monitoring health check results.   | Read         | -                           | -             | <ul style="list-style-type: none"> <li>ces:siteMonitorHealthCheck:get</li> </ul>       |
| ces:siteMonitorRule:createHealthCheck | Grants permission to create a website monitoring health check rule.   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>ces:siteMonitorHealthCheck:create</li> </ul>    |

| Action                                 | Description                                                          | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:netTopology:listRegion             | Grants permission to query the region where a tenant VPC is located. | List         | -                           | -             | -     |
| ces:netTopology:listVpc                | Grants permission to query the details of a tenant VPC in a region.  | List         | -                           | -             | -     |
| ces:netTopology:getVpcTopology         | Grants permission to query the topology of a tenant VPC.             | Read         | -                           | -             | -     |
| ces:netTopology:listRouteTableResource | Grants permission to query resources associated with a route table.  | List         | -                           | -             | -     |
| ces:qualityMonitor:listProbes          | Grants permission to list quality monitoring checkpoints.            | List         | -                           | -             | -     |
| ces:qualityMonitor:create              | Grants permission to create a quality monitoring task.               | Write        | -                           | -             | -     |
| ces:qualityMonitor:delete              | Grants permission to delete a quality monitoring task.               | Write        | -                           | -             | -     |

| Action                                      | Description                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:qualityMonitor:update                   | Grants permission to modify a quality monitoring task.                | Write        | -                           | -             | -     |
| ces:qualityMonitor:get                      | Grants permission to query details about a quality monitoring task.   | Read         | -                           | -             | -     |
| ces:qualityMonitor:list                     | Grants permission to list quality monitoring tasks.                   | List         | -                           | -             | -     |
| ces:qualityMonitor:listStatistics           | Grants permission to query quality monitoring statistics.             | List         | -                           | -             | -     |
| ces:qualityMonitor:queryMapStatus           | Grants permission to query map details.                               | List         | -                           | -             | -     |
| ces:qualityMonitor:queryMapThresholdConfig  | Grants permission to query map thresholds.                            | List         | -                           | -             | -     |
| ces:qualityMonitor:updateMapThresholdConfig | Grants permission to update thresholds of the quality monitoring map. | Write        | -                           | -             | -     |

| Action                                      | Description                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:qualityMonitor:getDetectionRecordDetail | Grants permission to query a detection record.                         | Read         | -                           | -             | -     |
| ces:qualityMonitor:listDetectionGroups      | Grants permission to list carriers or city groups.                     | List         | -                           | -             | -     |
| ces:qualityMonitor:listDetectionRecords     | Grants permission to list detection records of quality monitoring.     | List         | -                           | -             | -     |
| ces:paidContent:update                      | Grants permission to enable or disable commercial Cloud Eye functions. | Write        | -                           | -             | -     |
| ces:paidContent:list                        | Grants permission to list enabled commercial Cloud Eye functions.      | List         | -                           | -             | -     |
| ces:notificationObject:update               | Grants permission to modify a recipient.                               | Write        | -                           | -             | -     |
| ces:notificationPolicy:create               | Grants permission to create a notification policy.                     | Write        | -                           | -             | -     |

| Action                                       | Description                                                                                  | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:notificationPolicy:update                | Grants permission to update a notification policy.                                           | Write        | -                           | -             | -     |
| ces:notificationPolicy:get                   | Grants permission to query a notification policy.                                            | Read         | -                           | -             | -     |
| ces:notificationPolicy:list                  | Grants permission to list notification policies.                                             | List         | -                           | -             | -     |
| ces:notificationPolicy:delete                | Grants permission to delete a notification policy.                                           | Write        | -                           | -             | -     |
| ces:notificationPolicy:updateAlarmRelations  | Grants permission to update the association between a notification policy and an alarm rule. | Write        | -                           | -             | -     |
| ces:dashboard:listServiceResourcesStatistics | Grants permission to query resource statistics on a cloud service dashboard.                 | List         | -                           | ces:namespace | -     |
| ces:serviceProducts:list                     | Grants permission to batch query cloud service products.                                     | List         | -                           | -             | -     |

| Action                                  | Description                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:dashboard:listCloudServiceResources | Grants permission to list resources on a cloud service dashboard. | List         | -                           | ces:namespace | -     |
| ces:metric:createGroups                 | Grants permission to create a metric group.                       | Write        | -                           | -             | -     |
| ces:metric:listGroups                   | Grants permission to view a metric group.                         | List         | -                           | -             | -     |
| ces:metric:deleteGroups                 | Grants permission to delete a metric group.                       | Write        | -                           | -             | -     |
| ces:metric:updateGroups                 | Grants permission to update a metric group.                       | Write        | -                           | -             | -     |
| ces:metric:listConfig                   | Grants permission to obtain metric configurations.                | List         | -                           | -             | -     |
| ces:metric:createConfig                 | Grants permission to set metric configurations.                   | Write        | -                           | -             | -     |
| ces:alarms:publishNotification          | Grants permission to test alarm notifications.                    | Write        | -                           | -             | -     |

| Action                               | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:resourcesReportJob:create        | Grants permission to create a resource reporting task.                                     | Write        | -                           | -             | -     |
| ces:resourcesReportJob:list          | Grants permission to batch query resource reporting tasks.                                 | List         | -                           | -             | -     |
| ces:resourcesReportJob:delete        | Grants permission to batch delete resource reporting tasks.                                | Write        | -                           | -             | -     |
| ces:resourcesReportJob:download      | Grants permission to download a resource report.                                           | Read         | -                           | -             | -     |
| ces:agent:listSpecifiedProcResources | Grants permission to query custom process metrics.                                         | List         | -                           | -             | -     |
| ces:dashboard:listAlarmingResources  | Grants permission to query details about monitored resources on a cloud service dashboard. | List         | -                           | -             | -     |

| Action                                   | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:alarmHistory:update                  | Grants permission to modify a historical alarm.                                 | Write        | -                           | -             | -     |
| ces:alarmRulesReportJob:create           | Grants permission to batch create tasks for downloading alarm rules.            | Write        | -                           | -             | -     |
| ces:alarmRulesReportJob:list             | Grants permission to batch query tasks for downloading alarm rules.             | List         | -                           | -             | -     |
| ces:alarmRulesReportJob:delete           | Grants permission to batch delete tasks for downloading alarm rules.            | Write        | -                           | -             | -     |
| ces:alarmRulesReportJob:download         | Grants permission to download the alarm rule list.                              | Read         | -                           | -             | -     |
| ces:qualityMonitor:createQuickDetectTask | Grants permission to create an immediate detection task for quality monitoring. | Write        | -                           | -             | -     |



| Action                                       | Description                                                                                                              | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                       |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------------|
| ces:qualityMonitor:listQuickDetectTasks      | Grants permission to list immediate detection tasks of quality monitoring.                                               | List         | -                           | -             | -                                                                           |
| ces:qualityMonitor:showQuickDetectTaskDetail | Grants permission to query details about a single detection record in an immediate detection task of quality monitoring. | List         | -                           | -             | -                                                                           |
| ces:qualityMonitor:showQuickDetectTask       | Grants permission to query details about an immediate detection task of quality monitoring.                              | List         | -                           | -             | -                                                                           |
| ces::listServiceResources                    | Grants permission to list cloud service resources.                                                                       | List         | -                           | -             | <ul style="list-style-type: none"> <li>ces:serviceResources:list</li> </ul> |
| ces:alarmTemplates:list                      | Grants permission to batch query alarm templates.                                                                        | List         | -                           | -             | -                                                                           |
| ces:eventsBlackWhiteList:list                | Grants permission to query the event blacklist and whitelist.                                                            | List         | -                           | -             | -                                                                           |

| Action                                    | Description                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:eventsBlackWhiteList:update           | Grants permission to update the event blacklist and whitelist. | Write        | -                           | -             | -     |
| ces:metric:listMetaData                   | Grants permission to query metric metadata.                    | List         | -                           | -             | -     |
| ces:dataShareJob:listAgencyProjects       | Grants permission to list projects of a data dump delegator.   | List         | -                           | -             | -     |
| ces:dataShareJob:listDmsInstancesByAgency | Grants permission to list DMS instances of a delegator.        | List         | -                           | -             | -     |
| ces:dataShareJob:listDmsTopicsByAgency    | Grants permission to list DMS topics of a delegator.           | List         | -                           | -             | -     |
| ces:processMonitorTasks:list              | Grants permission to list process monitoring tasks.            | List         | -                           | -             | -     |
| ces:processMonitorTasks:create            | Grants permission to create a process monitoring task.         | Write        | -                           | -             | -     |
| ces:processMonitorTasks:get               | Grants permission to query a process monitoring task.          | Read         | -                           | -             | -     |

| Action                                | Description                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:processMonitorTasks:put           | Grants permission to update a process monitoring task. | Write        | -                           | -             | -     |
| ces:processMonitorTasks:delete        | Grants permission to delete a process monitoring task. | Write        | -                           | -             | -     |
| ces:dashboard:createMonitorDashboards | Grants permission to create a dashboard.               | Write        | -                           | -             | -     |
| ces:dashboard:listMonitorDashboards   | Grants permission to list dashboard templates.         | List         | -                           | -             | -     |
| ces:wecom:create                      | Grants permission to create a WeCom application.       | Write        | -                           | -             | -     |
| ces:wecom:update                      | Grants permission to update a WeCom application.       | Write        | -                           | -             | -     |
| ces:wecom:delete                      | Grants permission to delete a WeCom application.       | Write        | -                           | -             | -     |
| ces:wecom:list                        | Grants permission to list WeCom applications.          | List         | -                           | -             | -     |

| Action                             | Description                                                              | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:wecom:get                      | Grants permission to query a WeCom application.                          | Read         | -                           | -             | -     |
| ces:netTopology:listTenantEps      | Grants permission to query enterprise projects associated with a tenant. | List         | -                           | -             | -     |
| ces:netTopology:listGlobalTopology | Grants permission to query the global topology of a tenant.              | List         | -                           | -             | -     |
| ces:netDetection:listDetectRecords | Grants permission to query a tenant detection record.                    | List         | -                           | -             | -     |
| ces:netDetection:createDetectCase  | Grants permission to add a tenant detection case.                        | Write        | -                           | -             | -     |
| ces:netDetection:listDetectCases   | Grants permission to query a tenant detection case.                      | List         | -                           | -             | -     |
| ces:netDetection:updateDetectCase  | Grants permission to update a tenant detection case.                     | Write        | -                           | -             | -     |

| Action                                   | Description                                                    | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:netDetection:deleteDetectCase        | Grants permission to delete a tenant detection case.           | Write        | -                           | -             | -     |
| ces:netDetection:listDetectCaseReports   | Grants permission to query a tenant detection case report.     | List         | -                           | -             | -     |
| ces:netDetection:listAndCreateUploadCode | Grants permission to query and create an upload code.          | List         | -                           | -             | -     |
| ces:smartReportTask:create               | Grants permission to create an intelligent reporting task.     | Write        | -                           | -             | -     |
| ces:smartReportTask:list                 | Grants permission to query an intelligent reporting task.      | List         | -                           | -             | -     |
| ces:smartReportTask:update               | Grants permission to update an intelligent reporting task.     | Write        | -                           | -             | -     |
| ces:smartReportTask:delete               | Grants permission to batch delete intelligent reporting tasks. | Write        | -                           | -             | -     |

| Action                                    | Description                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| ces:smartReportTask:changeStatus          | Grants permission to batch enable or disable intelligent reporting tasks.             | Write        | -                           | -             | -     |
| ces:smartReportTask:listExecuteHistory    | Grants permission to query execution records of an intelligent reporting task.        | List         | -                           | -             | -     |
| ces:smartReportTask:downloadReportJob     | Grants permission to download an intelligent report.                                  | Read         | -                           | -             | -     |
| ces:smartReportTask:listSupportedServices | Grants permission to query cloud products supported by an intelligent reporting task. | List         | -                           | -             | -     |
| ces:smartReportJob:listResources          | Grants permission to list resources of an intelligent reporting task.                 | List         | -                           | -             | -     |
| ces:smartReportJob:show                   | Grants permission to query details about an intelligent reporting task.               | Read         | -                           | -             | -     |

Each API of Cloud Eye usually supports one or more actions. en-us\_topic\_0000001604910018.xml#EN-US\_TOPIC\_0000001604910018/EN-US\_TOPIC\_0000001604910018\_mMcCpPsS\_api\_relation\_table lists the supported actions and dependencies.

**Table 3-264** Actions and dependencies supported by Cloud Eye APIs

| API                                                            | Action                           | Dependencies |
|----------------------------------------------------------------|----------------------------------|--------------|
| POST /v2/{project_id}/alarms                                   | ces:alarms:create                | -            |
| POST /v2/{project_id}/alarms/batch-delete                      | ces:alarms:delete                | -            |
| POST /v2/{project_id}/alarms/action                            | ces:alarms:putAction             | -            |
| GET /v2/{project_id}/alarms                                    | ces:alarms:list                  | -            |
| POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-create | ces:alarms:addResources          | -            |
| POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-delete | ces:alarms:deleteResources       | -            |
| GET /v2/{project_id}/alarms/{alarm_id}/resources               | ces:alarms:getResources          | -            |
| PUT /v2/{project_id}/alarms/{alarm_id}/policies                | ces:alarms:updatePolicies        | -            |
| GET /v2/{project_id}/alarms/{alarm_id}/policies                | ces:alarms:getPolicies           | -            |
| PUT /v2/{project_id}/alarms/{alarm_id}/notifications           | ces:alarms:putAlarmNotifications | -            |

| API                                                                   | Action                                        | Dependencies |
|-----------------------------------------------------------------------|-----------------------------------------------|--------------|
| GET /v2/{project_id}/alarm-histories                                  | ces:alarmHistory:list                         | -            |
| POST /v2/{project_id}/alarm-templates                                 | ces:customAlarmTemplates:create               | -            |
| POST /v2/{project_id}/alarm-templates/batch-delete                    | ces:customAlarmTemplates:delete               | -            |
| PUT /v2/{project_id}/alarm-templates/{template_id}                    | ces:customAlarmTemplates:put                  | -            |
| GET /v2/{project_id}/alarm-templates                                  | ces:customAlarmTemplates:list                 | -            |
| GET /v2/{project_id}/alarm-templates/{template_id}                    | ces:customAlarmTemplates:get                  | -            |
| GET /v2/{project_id}/alarm-templates/{template_id}/association-alarms | ces:customAlarmTemplates:listAssociatedAlarms | -            |
| POST /v2/{project_id}/resource-groups                                 | ces:resourceGroups:create                     | -            |
| POST /v2/{project_id}/resource-groups/batch-delete                    | ces:resourceGroups:delete                     | -            |
| PUT /v2/{project_id}/resource-groups/{group_id}                       | ces:resourceGroups:put                        | -            |
| GET /v2/{project_id}/resource-groups/{group_id}                       | ces:resourceGroups:get                        | -            |



| API                                                                               | Action                                         | Dependencies |
|-----------------------------------------------------------------------------------|------------------------------------------------|--------------|
| GET /v2/{project_id}/resource-groups                                              | ces:resourceGroups:list                        | -            |
| PUT /v2/{project_id}/resource-groups/{group_id}/alarm-templates/async-association | ces:resourceGroups:putAssociationAlarmTemplate | -            |
| POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-create           | ces:resourceGroups:addResources                | -            |
| POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-delete           | ces:resourceGroups:deleteResources             | -            |
| GET /v2/{project_id}/resource-groups/{group_id}/services/{service}/resources      | ces:resourceGroups:getServiceResources         | -            |
| POST /v2/{project_id}/one-click-alarms                                            | ces:alarms:createOneClickAlarms                | -            |
| GET /v2/{project_id}/one-click-alarms                                             | ces:alarms:listOneClickAlarms                  | -            |
| GET /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms                 | ces:alarms:listOneClickAlarms                  | -            |
| PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarm-rules/action     | ces:alarms:putOneClickAlarms                   | -            |

| API                                                                                          | Action                                   | Dependencies |
|----------------------------------------------------------------------------------------------|------------------------------------------|--------------|
| POST /v2/{project_id}/one-click-alarms/batch-delete                                          | ces:alarms:deleteOneClickAlarms          | -            |
| PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/notifications                     | ces:alarms:putOneClickAlarmNotifications | -            |
| PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms/{alarm_id}/policies/action | ces:alarms:putOneClickAlarmPolicies      | -            |
| PUT /v2/{project_id}/notification-masks                                                      | ces:alarms:putNotificationMaskRules      | -            |
| POST /v2/{project_id}/notification-masks/batch-update                                        | ces:alarms:putNotificationMaskRules      | -            |
| PUT /v2/{project_id}/notification-masks/{notification_mask_id}                               | ces:alarms:putNotificationMaskRules      | -            |
| POST /v2/{project_id}/notification-masks/batch-delete                                        | ces:alarms:deleteNotificationMaskRules   | -            |
| POST /v2/{project_id}/notification-masks/batch-query                                         | ces:alarms:listNotificationMaskRules     | -            |
| GET /v2/{project_id}/notification-masks/{notification_mask_id}/resources                     | ces:alarms:listNotificationMaskResources | -            |
| POST /v2/{project_id}/dashboards                                                             | ces:dashboards:create                    | -            |

| API                                                           | Action                                       | Dependencies |
|---------------------------------------------------------------|----------------------------------------------|--------------|
| GET /v2/{project_id}/dashboards                               | ces:dashboards:list                          | -            |
| PUT /v2/{project_id}/dashboards/{dashboard_id}                | ces:dashboards:put                           | -            |
| POST /v2/{project_id}/dashboards/batch-delete                 | ces:dashboards:delete                        | -            |
| POST /v2/{project_id}/dashboards/{dashboard_id}/widgets       | ces:widgets:create                           | -            |
| GET /v2/{project_id}/dashboards/{dashboard_id}/widgets        | ces:widgets:list                             | -            |
| GET /v2/{project_id}/widgets/{widget_id}                      | ces:widgets:get                              | -            |
| DELETE /v2/{project_id}/widgets/{widget_id}                   | ces:widgets:delete                           | -            |
| POST /v2/{project_id}/widgets/batch-update                    | ces:widgets:put                              | -            |
| GET /v2/{project_id}/{resource_type}/tags                     | ces:tags:list                                | -            |
| GET /v2/{project_id}/instances/{instance_id}/agent-dimensions | ces:namespacesDimensions:listAgentDimensions | -            |
| POST /v2/{project_id}/batch-query-metric-data                 | ces:metricData:list                          | -            |

| API                                             | Action                | Dependencies |
|-------------------------------------------------|-----------------------|--------------|
| POST /V1.0/{project_id}/alarms                  | ces:alarms:create     | -            |
| PUT /V1.0/{project_id}/alarms/{alarm_id}        | ces:alarms:put        | -            |
| PUT /V1.0/{project_id}/alarms/{alarm_id}/action | ces:alarms:putAction  | -            |
| DELETE /V1.0/{project_id}/alarms/{alarm_id}     | ces:alarms:delete     | -            |
| GET /V1.0/{project_id}/alarms/{alarm_id}        | ces:alarms:get        | -            |
| GET /V1.0/{project_id}/alarms                   | ces:alarms:list       | -            |
| GET /V1.0/{project_id}/alarm-histories          | ces:alarmHistory:list | -            |
| POST /V1.0/{project_id}/events                  | ces:events:post       | -            |
| GET /V1.0/{project_id}/events                   | ces:events:list       | -            |
| GET /V1.0/{project_id}/event/{event_name}       | ces:events:get        | -            |
| GET /V1.0/{project_id}/metrics                  | ces:metrics:list      | -            |
| POST /V1.0/{project_id}/batch-query-metric-data | ces:metricData:list   | -            |
| GET /V1.0/{project_id}/event-data               | ces:eventData:get     | -            |
| GET /V1.0/{project_id}/metric-data              | ces:metricData:get    | -            |
| POST /V1.0/{project_id}/metric-data             | ces:metricData:create | -            |

| API                                                    | Action                          | Dependencies |
|--------------------------------------------------------|---------------------------------|--------------|
| GET /V1.0/{project_id}/quotas                          | ces:quotas:get                  | -            |
| GET /V1.0/{project_id}/resource-groups/{group_id}      | ces:resourceGroups:get          | -            |
| PUT /V1.0/{project_id}/resource-groups/{group_id}      | ces:resourceGroups:put          | -            |
| DELETE /V1.0/{project_id}/resource-groups/{group_id}   | ces:resourceGroups:delete       | -            |
| POST /V1.0/{project_id}/resource-groups                | ces:resourceGroups:create       | -            |
| GET /V1.0/{project_id}/resource-groups                 | ces:resourceGroups:list         | -            |
| POST /V1.0/{project_id}/alarm-template                 | ces:customAlarmTemplates:create | -            |
| PUT /V1.0/{project_id}/alarm-template/{template_id}    | ces:customAlarmTemplates:put    | -            |
| DELETE /V1.0/{project_id}/alarm-template/{template_id} | ces:customAlarmTemplates:delete | -            |
| GET /V1.0/{project_id}/alarm-template                  | ces:customAlarmTemplates:list   | -            |
| POST /v3/{project_id}/agent-status/batch-query         | ces:agent:listStatuses          | -            |
| GET /v3/{project_id}/agent-invocations                 | ces:agent:listTaskInvocations   | -            |

| API                                                  | Action                           | Dependencies |
|------------------------------------------------------|----------------------------------|--------------|
| POST /v3/{project_id}/agent-invocations/batch-create | ces:agent:createAgentInvocations | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [3](#), a resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for Cloud Eye.

**Table 3-265** Resource types supported by Cloud Eye

| Resource Type | URN                                                |
|---------------|----------------------------------------------------|
| alarm         | ces:<region>:<account-id>:alarm:<alarm-id>         |
| dashboard     | ces:<region>:<account-id>:dashboard:<dashboard-id> |

## Conditions

### About condition keys

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. It uses global condition keys applicable to all services but excludes **g:RequestedRegion**. For details, see [Global Condition Keys](#).

#### NOTE

Cloud Eye provides global capabilities (such as **Alarm Notifications** and **Task Center**). As a result, it functions as a global-level service and does not support the global condition key **g:RequestedRegion**.

- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, ces:) apply only to operations of EVS. For details, see [Table 3-266](#).

- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

### Service-specific condition keys supported by Cloud Eye

The following table lists the condition keys that you can define in custom identity policies for Cloud Eye. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-266** Service-specific condition keys supported by Cloud Eye

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                                                                                 |
|--------------------------------|--------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ces:namespace</code>     | string | Multi-value                   | Filters access requests based on the namespace specified in the request parameter. For details, see <a href="#">Granting Permissions by Cloud Service</a> . |

## 3.14.9 Simple Message Notification (SMN)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by SMN, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by SMN, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for SMN.



**Table 3-267** Actions supported by SMN

| Action                | Description                                | Access Level | Resource Type (*: Mandatory) | Condition Key                                                                                                                                                                          | Alias                                                                |
|-----------------------|--------------------------------------------|--------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| smn:topic:create      | Grants permissions to create a topic.      | Write        | topic *                      | N/A                                                                                                                                                                                    | N/A                                                                  |
|                       |                                            |              | N/A                          | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                                                                      |
| smn:topic:listTopic   | Grants permissions to query topics.        | List         | topic *                      | N/A                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>• smn:topic:list</li> </ul>   |
|                       |                                            |              | N/A                          | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                  |                                                                      |
| smn:topic:updateTopic | Grants permissions to update a topic.      | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• smn:topic:update</li> </ul> |
| smn:topic:get         | Grants permissions to query topic details. | Read         | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | <ul style="list-style-type: none"> <li>• smn:topic:list</li> </ul>   |
| smn:topic:delete      | Grants permissions to delete a topic.      | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                                     | N/A                                                                  |

| Action                    | Description                                          | Access Level | Resource Type (*: Mandatory) | Condition Key                                                                                                                                                                   | Alias                                                                |
|---------------------------|------------------------------------------------------|--------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| smn:topic:listAttributes  | Grants permissions to query a topic policy.          | List         | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                              | <ul style="list-style-type: none"> <li>• smn:topic:list</li> </ul>   |
| smn:topic:deleteAttribute | Grants permissions to delete a topic policy.         | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                              | <ul style="list-style-type: none"> <li>• smn:topic:update</li> </ul> |
| smn:topic:updateAttribute | Grants permissions to update a topic policy.         | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                              | <ul style="list-style-type: none"> <li>• smn:topic:update</li> </ul> |
|                           |                                                      |              | N/A                          | <ul style="list-style-type: none"> <li>• <a href="#">smn:TargetOrgPath</a></li> <li>• <a href="#">smn:TargetOrgId</a></li> <li>• <a href="#">smn:TargetAccountId</a></li> </ul> |                                                                      |
| smn:topic:subscribe       | Grants permissions to add a subscription to a topic. | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul>                              | <ul style="list-style-type: none"> <li>• smn:topic:update</li> </ul> |
|                           |                                                      |              | N/A                          | <ul style="list-style-type: none"> <li>• <a href="#">smn:Protocol</a></li> <li>• <a href="#">smn:Endpoint</a></li> </ul>                                                        |                                                                      |

| Action                             | Description                                               | Access Level | Resource Type (*: Mandatory) | Condition Key                                                                                                                                      | Alias                                                                 |
|------------------------------------|-----------------------------------------------------------|--------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| smn:topic:listSubscriptionsByTopic | Grants permissions to query subscriptions of a topic.     | List         | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• smn:topic:list</li> </ul>    |
| smn:topic:listSubscriptions        | Grants permissions to query subscriptions of all topics.  | List         | topic *                      | N/A                                                                                                                                                | <ul style="list-style-type: none"> <li>• smn:topic:list</li> </ul>    |
| smn:topic:deleteSubscription       | Grants permissions to delete a subscription from a topic. | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• smn:topic:update</li> </ul>  |
| smn:topic:updateSubscription       | Grants permissions to update a subscription of a topic.   | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• smn:topic:update</li> </ul>  |
| smn:topic:publish                  | Grants permissions to publish a message.                  | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | N/A                                                                   |
| smn:template:create                | Grants permissions to create a message template.          | Write        | template *                   | N/A                                                                                                                                                | N/A                                                                   |
| smn:template:listTemplates         | Grants permissions to query message templates.            | List         | template *                   | N/A                                                                                                                                                | <ul style="list-style-type: none"> <li>• smn:template:list</li> </ul> |

| Action              | Description                                                | Access Level | Resource Type (*: Mandatory) | Condition Key                                                                                                                                  | Alias                                                               |
|---------------------|------------------------------------------------------------|--------------|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| smn:template:update | Grants permissions to modify a message template.           | Write        | template *                   | N/A                                                                                                                                            | N/A                                                                 |
| smn:template:get    | Grants permissions to query details of a message template. | Read         | template *                   | N/A                                                                                                                                            | <ul style="list-style-type: none"> <li>smn:template:list</li> </ul> |
| smn:template:delete | Grants permissions to delete a message template.           | Write        | template *                   | N/A                                                                                                                                            | N/A                                                                 |
| smn:tag:create      | Grants permissions to add a tag for a topic.               | Write        | topic *                      | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | N/A                                                                 |
|                     |                                                            |              | N/A                          | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              |                                                                     |
| smn:tag:delete      | Grants permissions to delete a tag of a topic.             | Write        | topic *                      | <ul style="list-style-type: none"> <li><a href="#">g:EnterpriseProjectId</a></li> <li><a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>smn:tag:update</li> </ul>    |
|                     |                                                            |              | N/A                          | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul>              |                                                                     |

| Action                  | Description                                                                        | Access Level | Resource Type (*: Mandatory) | Condition Key                                                                                                                                      | Alias              |
|-------------------------|------------------------------------------------------------------------------------|--------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| smn:tag:batchModify     | Grants permissions to batch modify topic tags.                                     | Write        | topic*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • smn:tag:update   |
|                         |                                                                                    |              | N/A                          | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul>              |                    |
| smn:tag:list            | Grants permissions to query tags of a topic.                                       | Read         | topic*                       | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                      | N/A                |
| smn:topic:createLogTank | Grants permissions to associate a topic with a log group and log stream.           | Write        | topic*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | N/A                |
| smn:topic:listLogTank   | Grants permissions to query the log group and log stream associated with a topic.  | List         | topic*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • smn:topic:list   |
| smn:topic:updateLogTank | Grants permissions to update the log group and log stream associated with a topic. | Write        | topic*                       | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | • smn:topic:update |

| Action                       | Description                                                                 | Access Level | Resource Type (*: Mandatory) | Condition Key                                                                                                                                      | Alias                                                                |
|------------------------------|-----------------------------------------------------------------------------|--------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| smn:topic:deleteLogTank      | Grants permissions to disassociate a topic from a log group and log stream. | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | <ul style="list-style-type: none"> <li>• smn:topic:update</li> </ul> |
| smn:topic:createKmsKey       | Grants permissions to bind a KMS key to a topic.                            | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | N/A                                                                  |
| smn:topic:getKmsKey          | Grants permissions to query the KMS key bound to a topic.                   | List         | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | N/A                                                                  |
| smn:topic:updateKmsKey       | Grants permissions to update the KMS key bound to a topic.                  | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | N/A                                                                  |
| smn:topic:deleteKmsKey       | Grants permissions to delete the KMS key bound to a topic.                  | Write        | topic *                      | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">g:ResourceTag/&lt;tag-key&gt;</a></li> </ul> | N/A                                                                  |
| smn:topic:createNotifyPolicy | Grants permissions to create a notification policy.                         | Write        | topic *                      | N/A                                                                                                                                                | N/A                                                                  |

| Action                       | Description                                               | Access Level | Resource Type (*: Mandatory) | Condition Key | Alias |
|------------------------------|-----------------------------------------------------------|--------------|------------------------------|---------------|-------|
| smn:topic:updateNotifyPolicy | Grants permissions to modify a notification policy.       | Write        | topic *                      | N/A           | N/A   |
| smn:topic:getNotifyPolicy    | Grants permissions to query a notification policy.        | Read         | topic *                      | N/A           | N/A   |
| smn:topic:deleteNotifyPolicy | Grants permissions to delete a notification policy.       | Write        | topic *                      | N/A           | N/A   |
| smn:application:create       | Grants permissions to create an application.              | Write        | application *                | N/A           | N/A   |
| smn:application:delete       | Grants permissions to delete an application.              | Write        | application *                | N/A           | N/A   |
| smn:application:list         | Grants permissions to query an application.               | List         | application *                | N/A           | N/A   |
| smn:application:get          | Grants permissions to query application details.          | Read         | application *                | N/A           | N/A   |
| smn:application:publish      | Grants permissions to publish messages of an application. | Write        | application *                | N/A           | N/A   |

| Action                         | Description                                    | Access Level | Resource Type (*: Mandatory) | Condition Key                                                                                                            | Alias |
|--------------------------------|------------------------------------------------|--------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------|
| smn:application:createPlatform | Grants permissions to create a platform.       | Write        | application *                | N/A                                                                                                                      | N/A   |
| smn:application:deletePlatform | Grants permissions to delete a platform.       | Write        | application *                | N/A                                                                                                                      | N/A   |
| smn:application:updatePlatform | Grants permissions to update a platform.       | Write        | application *                | N/A                                                                                                                      | N/A   |
| smn:application:listPlatform   | Grants permissions to query the platform list. | List         | application *                | N/A                                                                                                                      | N/A   |
| smn:application:getPlatform    | Grants permissions to query platform details.  | Read         | application *                | N/A                                                                                                                      | N/A   |
| smn:subscriptionUser:create    | Grants permissions to create a subscriber.     | Write        | subscription_user *          | N/A                                                                                                                      | N/A   |
|                                |                                                |              | N/A                          | <ul style="list-style-type: none"> <li>• <a href="#">smn:Protocol</a></li> <li>• <a href="#">smn:Endpoint</a></li> </ul> |       |
| smn:subscriptionUser:delete    | Grants permissions to delete a subscriber.     | Write        | subscription_user *          | N/A                                                                                                                      | N/A   |
| smn:subscriptionUser:update    | Grants permissions to update a subscriber.     | Write        | subscription_user *          | N/A                                                                                                                      | N/A   |



| Action                    | Description                                      | Access Level | Resource Type (*: Mandatory) | Condition Key | Alias |
|---------------------------|--------------------------------------------------|--------------|------------------------------|---------------|-------|
| smn:subscriptionUser:list | Grants permissions to query the subscriber list. | List         | subscription_user*           | N/A           | N/A   |

Each API of SMN usually supports one or more actions. [Table 3-268](#) lists the supported actions and dependencies.

**Table 3-268** Actions and dependencies supported by SMN APIs

| API                                                              | Action                   | Dependency |
|------------------------------------------------------------------|--------------------------|------------|
| POST /v2/{project_id}/notifications/topics                       | smn:topic:create         | N/A        |
| GET /v2/{project_id}/notifications/topics                        | smn:topic:listTopic      | N/A        |
| PUT /v2/{project_id}/notifications/topics/{topic_urn}            | smn:topic:updateTopic    | N/A        |
| GET /v2/{project_id}/notifications/topics/{topic_urn}            | smn:topic:get            | N/A        |
| DELETE /v2/{project_id}/notifications/topics/{topic_urn}         | smn:topic:delete         | N/A        |
| GET /v2/{project_id}/notifications/topics/{topic_urn}/attributes | smn:topic:listAttributes | N/A        |

| API                                                                                                        | Action                                  | Dependency |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------|------------|
| DELETE /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>attributes                        | smn:topic:deleteAttribute               | N/A        |
| PUT /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>attributes/{name}                    | smn:topic:updateAttribute               | N/A        |
| DELETE /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>attributes/{name}                 | smn:topic:deleteAttribute               | N/A        |
| POST /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>subscriptions                       | smn:topic:subscribe                     | N/A        |
| GET /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>subscriptions                        | smn:topic:listSubscriptions-<br>ByTopic | N/A        |
| PUT /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>subscriptions/<br>{subscription_urn} | smn:topic:updateSubscription            | N/A        |
| DELETE /v2/<br>{project_id}/<br>notifications/<br>subscriptions/<br>{subscription_urn}                     | smn:topic:deleteSubscription            | N/A        |
| DELETE /v2/<br>{project_id}/<br>notifications/<br>subscriptions                                            | smn:topic:deleteSubscription            | N/A        |

| API                                                                                                           | Action                       | Dependency |
|---------------------------------------------------------------------------------------------------------------|------------------------------|------------|
| DELETE /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>subscriptions/<br>{subscription_urn} | smn:topic:deleteSubscription | N/A        |
| DELETE /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>subscriptions                        | smn:topic:deleteSubscription | N/A        |
| GET /v2/<br>{project_id}/<br>notifications/<br>subscriptions                                                  | smn:topic:listSubscriptions  | N/A        |
| POST /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/publish                                    | smn:topic:publish            | N/A        |
| POST /v2/<br>{project_id}/<br>notifications/<br>message_template                                              | smn:template:create          | N/A        |
| GET /v2/<br>{project_id}/<br>notifications/<br>message_template                                               | smn:template:listTemplates   | N/A        |
| PUT /v2/<br>{project_id}/<br>notifications/<br>message_template/<br>{message_template<br>_id}                 | smn:template:update          | N/A        |
| GET /v2/<br>{project_id}/<br>notifications/<br>message_template/<br>{message_template<br>_id}                 | smn:template:get             | N/A        |
| DELETE /v2/<br>{project_id}/<br>notifications/<br>message_template/<br>{message_template<br>_id}              | smn:template:delete          | N/A        |

| API                                                                                             | Action                  | Dependency                                                                                   |
|-------------------------------------------------------------------------------------------------|-------------------------|----------------------------------------------------------------------------------------------|
| POST /v2/<br>{project_id}/<br>{resource_type}/<br>{resource_id}/tags                            | smn:tag:create          | N/A                                                                                          |
| GET /v2/<br>{project_id}/<br>{resource_type}/<br>{resource_id}/tags                             | smn:tag:list            | N/A                                                                                          |
| POST /v2/<br>{project_id}/<br>{resource_type}/<br>{resource_id}/tags/<br>action                 | smn:tag:batchModify     | <ul style="list-style-type: none"> <li>• smn:tag:create</li> <li>• smn:tag:delete</li> </ul> |
| DELETE /v2/<br>{project_id}/<br>{resource_type}/<br>{resource_id}/tags/<br>{key}                | smn:tag:delete          | N/A                                                                                          |
| GET /v2/<br>{project_id}/<br>{resource_type}/<br>tags                                           | smn:tag:list            | N/A                                                                                          |
| POST /v2/<br>{project_id}/<br>{resource_type}/<br>resource_instances/<br>action                 | smn:tag:list            | N/A                                                                                          |
| GET /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>logtanks                  | smn:topic:listLogTank   | N/A                                                                                          |
| POST /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>logtanks                 | smn:topic:createLogTank | N/A                                                                                          |
| PUT /v2/<br>{project_id}/<br>notifications/topics/<br>{topic_urn}/<br>logtanks/<br>{logtank_id} | smn:topic:updateLogTank | N/A                                                                                          |

| API                                                                                          | Action                       | Dependency                          |
|----------------------------------------------------------------------------------------------|------------------------------|-------------------------------------|
| DELETE /v2/{project_id}/notifications/topics/{topic_urn}/logtanks/{logtank_id}               | smn:topic:deleteLogTank      | N/A                                 |
| POST /v2/{project_id}/notifications/subscriptions/filter_policies                            | smn:topic:updateSubscription | N/A                                 |
| PUT /v2/{project_id}/notifications/subscriptions/filter_policies                             | smn:topic:updateSubscription | N/A                                 |
| DELETE /v2/{project_id}/notifications/subscriptions/filter_policies                          | smn:topic:updateSubscription | N/A                                 |
| POST /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions/from-subscription-users | smn:topic:subscribe          | N/A                                 |
| POST /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy                         | smn:topic:createNotifyPolicy | smn:topic:listSubscriptions-ByTopic |
| PUT /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id}       | smn:topic:updateNotifyPolicy | smn:topic:listSubscriptions-ByTopic |
| GET /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy                          | smn:topic:getNotifyPolicy    | N/A                                 |

| API                                                                                       | Action                         | Dependency                                                                                   |
|-------------------------------------------------------------------------------------------|--------------------------------|----------------------------------------------------------------------------------------------|
| DELETE /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id} | smn:topic:deleteNotifyPolicy   | N/A                                                                                          |
| GET /v2/{project_id}/notifications/topics/{topic_urn}/statistics                          | smn:topic:get                  | N/A                                                                                          |
| POST /v2/{project_id}/notifications/topics/{topic_urn}/kms                                | smn:topic:createKmsKey         | smn:topic:get                                                                                |
| PUT /v2/{project_id}/notifications/topics/{topic_urn}/kms/{id}                            | smn:topic:updateKmsKey         | <ul style="list-style-type: none"> <li>smn:topic:get</li> <li>smn:topic:getKmsKey</li> </ul> |
| GET /v2/{project_id}/notifications/topics/{topic_urn}/kms                                 | smn:topic:getKmsKey            | smn:topic:get                                                                                |
| DELETE /v2/{project_id}/notifications/topics/{topic_urn}/kms/{id}                         | smn:topic:deleteKmsKey         | <ul style="list-style-type: none"> <li>smn:topic:get</li> <li>smn:topic:getKmsKey</li> </ul> |
| N/A                                                                                       | smn:application:create         | N/A                                                                                          |
| N/A                                                                                       | smn:application:delete         | N/A                                                                                          |
| N/A                                                                                       | smn:application:list           | N/A                                                                                          |
| N/A                                                                                       | smn:application:get            | N/A                                                                                          |
| N/A                                                                                       | smn:application:publish        | N/A                                                                                          |
| N/A                                                                                       | smn:application:createPlatform | N/A                                                                                          |
| N/A                                                                                       | smn:application:deletePlatform | N/A                                                                                          |
| N/A                                                                                       | smn:application:updatePlatform | N/A                                                                                          |
| N/A                                                                                       | smn:application:listPlatform   | N/A                                                                                          |

| API                                                        | Action                      | Dependency |
|------------------------------------------------------------|-----------------------------|------------|
| N/A                                                        | smn:application:getPlatform | N/A        |
| POST /v2/<br>{domain_id}/<br>subscription-users            | smn:subscriptionUser:create | N/A        |
| DELETE /v2/<br>{domain_id}/<br>subscription-users/<br>{id} | smn:subscriptionUser:delete | N/A        |
| PUT /v2/<br>{domain_id}/<br>subscription-users/<br>{id}    | smn:subscriptionUser:update | N/A        |
| GET /v2/<br>{domain_id}/<br>subscription-users             | smn:subscriptionUser:list   | N/A        |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-269](#), a resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for SMN.

**Table 3-269** Resource types supported by SMN

| Resource Type     | URN                                                        |
|-------------------|------------------------------------------------------------|
| application       | smn::<account-id>:application:<application-id>             |
| topic             | smn:<region>:<account-id>:topic:<topic-id>                 |
| subscription_user | smn::<account-id>:subscription_user:<subscription-user-id> |
| template          | smn:<region>:<account-id>:template:<template-id>           |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, smn:) only apply to operations of the SMN service. For details, see [Table 3-270](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

#### Service-specific condition keys supported by SMN

The following table lists the condition keys that you can define in custom identity policies for SMN. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-270** Service-specific condition keys supported by SMN

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                         |
|--------------------------------|--------|-------------------------------|-----------------------------------------------------|
| smn:TargetOrgPath              | string | Single-valued                 | The organization path authorized in a topic policy. |
| smn:TargetOrgId                | string | Single-valued                 | The organization ID authorized in a topic policy.   |
| smn:TargetAccountId            | string | Single-valued                 | The account ID authorized in a topic policy.        |
| smn:Protocol                   | string | Single-valued                 | The subscription protocol.                          |
| smn:Endpoint                   | string | Single-valued                 | The subscription endpoint address.                  |



### 3.14.10 Log Tank Service (LTS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by LTS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by LTS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for LTS.

**Table 3-271** Actions supported by LTS

| Action                        | Description                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias                                                                                         |
|-------------------------------|-------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| lts:logGroup:deleteLogGroup   | Grants permission to delete log group.    | Write        | logGroup *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:groups:delete</li> </ul>                         |
| lts:logGroup:listLogGroup     | Grants permission to get log group list.  | List         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• lts:groups:get</li> <li>• lts:groups:list</li> </ul> |
| lts:logGroup:createLogGroup   | Grants permission to create log group.    | Write        | logGroup *                  | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• lts:groups:create</li> </ul>                         |
|                               |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                                                                                               |
| lts:logGroup:updateLogGroup   | Grants permission to update log group.    | Write        | logGroup *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:groups:put</li> </ul>                            |
|                               |                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                                                                                               |
| lts:logStream:listLogStream   | Grants permission to get log stream list. | List         | logGroup *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:topics:get</li> <li>• lts:topics:list</li> </ul> |
| lts:logStream:deleteLogStream | Grants permission to delete log stream.   | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:topics:delete</li> </ul>                         |

| Action                           | Description                                 | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                    | Alias                                                                                                            |
|----------------------------------|---------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| lts:logStream:createLogStream    | Grants permission to create log stream.     | Write        | logGroup *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>                                              |
|                                  |                                             |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> <li><a href="#">g:EnterpriseProjectId</a></li> </ul> |                                                                                                                  |
| lts:logStream:searchLog          | Grants permission to get logs list.         | List         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | <ul style="list-style-type: none"> <li>lts:logs:list</li> </ul>                                                  |
| lts:logStream:searchStructLog    | Grants permission to get struct logs list.  | List         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | <ul style="list-style-type: none"> <li>lts:topics:list</li> <li>lts:topics:get</li> <li>lts:logs:list</li> </ul> |
| lts:logStream:searchLogHistogram | Grants permission to get logHistogram list. | List         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                    | <ul style="list-style-type: none"> <li>lts:topics:list</li> <li>lts:sqlalarmrules:create</li> </ul>              |
| lts:transfer:createTransfer      | Grants permission to create transfer.       | Write        | -                           | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>lts:transfer:create</li> </ul>                                            |
| lts:transfer:deleteTransfer      | Grants permission to delete transfer.       | Write        | transfer *                  | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>lts:transfer:delete</li> </ul>                                            |
| lts:transfer:listTransfer        | Grants permission to get transfers list.    | List         | -                           | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>lts:transfer:list</li> </ul>                                              |
| lts:transfer:updateTransfer      | Grants permission to update transfer.       | Write        | transfer *                  | -                                                                                                                                                                                | <ul style="list-style-type: none"> <li>lts:transfer:put</li> </ul>                                               |

| Action                                   | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                                |
|------------------------------------------|--------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------------------------------------|
| lts:transfer:registerDmsKafkaInstance    | Grants permission to register DmsKafka instance. | Write        | -                           | -                                             | -                                                                                                    |
| lts:configCenter:updateOverCollectSwitch | Grants permission to update over collect switch. | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>aom:quota:set</li> </ul>                                      |
| lts:structConfig:createStructConfig      | Grants permission to create struct config.       | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:create</li> <li>lts:structConfig:create</li> </ul> |
| lts:structConfig:deleteStructConfig      | Grants permission to delete struct config.       | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:structConfig:delete</li> </ul>                            |
| lts:structConfig:getStructConfig         | Grants permission to get struct config.          | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:get</li> <li>lts:structConfig:get</li> </ul>       |
| lts:structConfig:listStructTemplate      | Grants permission to get struct template list.   | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>                                     |
| lts:structConfig:updateStructConfig      | Grants permission to update struct config.       | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:put</li> <li>lts:structConfig:put</li> </ul>       |
| lts:mappingRule:create                   | Grants permission to create mapping rule.        | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>                                  |
| lts:mappingRule:delete                   | Grants permission to delete mapping rule.        | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>                                  |

| Action                           | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias                                                                      |
|----------------------------------|--------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| lts:mappingRule:get              | Grants permission to get mapping rule detail.    | Read         | -                           | -                                                                                                                                 | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>           |
| lts:mappingRule:list             | Grants permission to get mapping rule list.      | List         | -                           | -                                                                                                                                 | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>           |
| lts:mappingRule:update           | Grants permission to update mapping rule.        | Write        | -                           | -                                                                                                                                 | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>           |
| lts:logStream:getHistorySql      | Grants permission to get log stream history sql. | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>           |
| lts:alarmRule:createSqlAlarmRule | Grants permission to create sql alarm rules.     | Write        | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:create</li> </ul> |
| lts:alarmRule:deleteSqlAlarmRule | Grants permission to delete sql alarm rules.     | Write        | alarmRule *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:delete</li> </ul> |
| lts:alarmRule:updateSqlAlarmRule | Grants permission to update sql alarm rules.     | Write        | alarmRule *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:put</li> </ul>    |
|                                  |                                                  |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                                                                            |
| lts:alarmRule:listSqlAlarmRule   | Grants permission to get sql alarm rules.        | List         | -                           | -                                                                                                                                 | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul>    |

| Action                               | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias                      |
|--------------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| lts:alarmRule:createWordAlarmRule    | Grants permission to create word alarm rules.              | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> | • lts:sqlalarmrules:create |
| lts:alarmRule:deleteWordAlarmRule    | Grants permission to delete word alarm rules.              | Write        | alarm Rule *                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | • lts:sqlalarmrules:delete |
| lts:alarmRule:updateWordAlarmRule    | Grants permission to update word alarm rules.              | Write        | alarm Rule *                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | • lts:sqlalarmrules:put    |
|                                      |                                                            |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                            |
| lts:alarmRule:listWordAlarmRule      | Grants permission to get word alarm rules.                 | List         | -                           | -                                                                                                                                     | -                          |
| lts:alarm:cleanAlarm                 | Grants permission to delete alarm.                         | Write        | -                           | -                                                                                                                                     | • lts:sqlalarmrules:delete |
| lts:alarm:listAlarm                  | Grants permission to get alarm list.                       | List         | -                           | -                                                                                                                                     | • lts:sqlalarmrules:get    |
| lts:logStream:listChart              | Grants permission to query the log stream chart.           | List         | -                           | -                                                                                                                                     | -                          |
| lts:alarmNotificationTemplate:create | Grants permission to creating alarm notification template. | Write        | -                           | -                                                                                                                                     | • lts:sqlalarmrules:create |
| lts:alarmNotificationTemplate:update | Grants permission to update alarm notification template.   | Write        | -                           | -                                                                                                                                     | • lts:sqlalarmrules:put    |

| Action                               | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                      |
|--------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------|
| lts:alarmNotificationTemplate:delete | Grants permission to delete alarm notification template.        | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:delete</li> </ul> |
| lts:alarmNotificationTemplate:list   | Grants permission to query alarm notification template list.    | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul>    |
| lts:alarmNotificationTemplate:get    | Grants permission to query alarm notification template details. | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul>    |
| lts:hostGroup:create                 | Grants permission to create host group.                         | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>        |
| lts:hostGroup:delete                 | Grants permission to delete Host Group.                         | Write        | hostGroup *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>        |
| lts:hostGroup:list                   | Grants permission to query host group list.                     | List         | -                           | -                                             | -                                                                          |
| lts:hostGroup:list                   | Grants permission to query host group list.                     | List         | accessConfig *              | -                                             | <ul style="list-style-type: none"> <li>lts:topics:list</li> </ul>          |
| lts:hostGroup:update                 | Grants permission to update host group list.                    | Write        | hostGroup *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>           |
| lts:accessConfig:create              | Grants permission to create access config.                      | Write        | logStream *                 | -                                             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>        |

| Action                  | Description                                  | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias                                                                     |
|-------------------------|----------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| lts:accessConfig:delete | Grants permission to delete access config.   | Write        | accessConfig *              | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                                                                         |
| lts:accessConfig:list   | Grants permission to get access config list. | List         | -                           | -                                                                                                                                 | <ul style="list-style-type: none"> <li>lts:topics:list</li> </ul>         |
| lts:accessConfig:update | Grants permission to update access config.   | Write        | accessConfig *              | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>          |
|                         |                                              |              | hostGroup                   | -                                                                                                                                 |                                                                           |
| lts:tag:create          | Grants permission to create or update tag.   | Tagging      | logGroup                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | <ul style="list-style-type: none"> <li>lts:resourceTags:put</li> </ul>    |
|                         |                                              |              | logStream                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                           |
|                         |                                              |              | accessConfig                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                           |
|                         |                                              |              | hostGroup                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                           |
|                         |                                              |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                                                                           |
| lts:tag:delete          | Grants permission to delete tag.             | Tagging      | logGroup                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | <ul style="list-style-type: none"> <li>lts:resourceTags:delete</li> </ul> |
|                         |                                              |              | logStream                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                           |
|                         |                                              |              | accessConfig                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                           |
|                         |                                              |              | hostGroup                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     |                                                                           |



| Action                         | Description                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias                                                                                                           |
|--------------------------------|---------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
|                                |                                                   |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |                                                                                                                 |
| lts:logStream:createQuickQuery | Grants permission to create quick query.          | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:searchcriteria:create</li> <li>• lts:searchcriteria:put</li> </ul> |
| lts:logStream:deleteQuickQuery | Grants permission to delete quick query.          | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:searchcriteria:delete</li> </ul>                                   |
| lts:logStream:listQuickQuery   | Grants permission to query quick query list.      | List         | logGroup *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:searchcriteria:list</li> </ul>                                     |
| lts:logFavorite:create         | Grants permission to create log favorite.         | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:topics:create</li> </ul>                                           |
| lts:logFavorite:delete         | Grants permission to delete log favorite.         | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | <ul style="list-style-type: none"> <li>• lts:topics:delete</li> </ul>                                           |
| lts:dashboardGroup:create      | Grants permission to create dashboard group.      | Write        | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• lts:topics:create</li> </ul>                                           |
| lts:dashboard:create           | Grants permission to create dashboard.            | Write        | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• lts:topics:create</li> </ul>                                           |
| lts:trafficStatistic:get       | Grants permission to get trafficStatistic detail. | Read         | -                           | -                                                                                                                                     | <ul style="list-style-type: none"> <li>• lts:logs:list</li> </ul>                                               |

| Action                | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                                  |
|-----------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------------------|
| lts:tokenizer:get     | Grants permission to obtains the configured separator.                                     | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:get</li> <li>aom:log:list</li> </ul> |
| lts:tokenizer:create  | Grants permission to preview Word Breakers.                                                | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>                       |
| lts:tokenizer:preview | Grants permission to preview Word Breakers.                                                | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> <li>aom:log:list</li> </ul> |
| lts:usageAlarm:update | Grants permission to enables or disables usage warning.                                    | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>                       |
| lts:csvTable:list     | Grants permission to obtaining the Associated Data Source Configuration Information Table. | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:list</li> </ul>               |
| lts:csvTable:upload   | Grants permission to uploading a CSV File.                                                 | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:create</li> </ul>             |
| lts:csvTable:get      | Grants permission to preview associated data and view associated data source information.  | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul>                |

| Action                  | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                      |
|-------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------|
| lts:csvTable:create     | Grants permission to creating Associated Data Sources.                            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:create</li> </ul> |
| lts:csvTable:update     | Grants permission to updating Associated Data Sources.                            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:put</li> </ul>    |
| lts:csvTable:delete     | Grants permission to deleting Associated Data Sources.                            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:delete</li> </ul> |
| lts:scheduledSql:create | Grants permission to create a scheduled SQL statement.                            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:create</li> </ul> |
| lts:scheduledSql:delete | Grants permission to delete the scheduled SQL statement.                          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:delete</li> </ul> |
| lts:scheduledSql:update | Grants permission to modify the scheduled SQL statement.                          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:put</li> </ul>    |
| lts:scheduledSql:list   | Grants permission to get this interface is used to obtain the scheduled SQL list. | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:list</li> </ul>   |

| Action                              | Description                                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                      |
|-------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------------|
| lts:scheduledSql:get                | Grants permission to get scheduled SQL details.                                    | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul>    |
| lts:scheduledSql:retry              | Grants permission to retry the execution instance.                                 | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:delete</li> </ul> |
| lts:transfer:getDisList             | Grants permission to obtaining the dis channel list.                               | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:disStreams:list</li> </ul>      |
| lts:transfer:listKafkaInstance      | Grants permission to obtaining the Kafka List.                                     | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:kafka:list</li> </ul>           |
| lts:transfer:updateKafkaInstance    | Grants permission to updating kafka information.                                   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:kafka:update</li> </ul>         |
| lts:transfer:deleteKafkaInstance    | Grants permission to deleting kafka information.                                   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:kafka:delete</li> </ul>         |
| lts:transfer:listKafkaAuthorization | Grants permission to querying the kafka authorization list of user configurations. | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:kafka:list</li> </ul>           |

| Action                                | Description                                                                  | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                 |
|---------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------------------------------|
| lts:transfer:createKafkaAuthorization | Grants permission to adding a user configuration kafka authorization list.   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:kafka:create</li> </ul>    |
| lts:transfer:deleteKafkaAuthorization | Grants permission to deleting a user configuration kafka authorization list. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:kafka:delete</li> </ul>    |
| lts:transfer:getTransfer              | Grants permission to obtaining information about a dump task.                | Read         | transfer *                  | -             | <ul style="list-style-type: none"> <li>lts:transfer:list</li> </ul>   |
| lts:transfer:getDwsInfo               | Grants permission to querying dws information of a tenant.                   | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:transfer:list</li> </ul>   |
| lts:transfer:registerDwsCluster       | Grants permission to registering a dws cluster.                              | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:transfer:create</li> </ul> |
| lts:hostGroup:getHost                 | Grants permission to obtains all hosts based on query conditions..           | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:list</li> </ul>     |

| Action                   | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                       |
|--------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|---------------------------------------------------------------------------------------------|
| lts:hostGroup:get        | Grants permission to obtains all configurations of a single host group based on search criteria. | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:list</li> </ul>                           |
| lts:accessConfig:get     | Grants permission to obtaining a single collection configuration.                                | Read         | accessConfig *              | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>                            |
| lts:logFavorite:list     | Grants permission to obtaining the favorites list.                                               | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>                            |
| lts:logFavorite:update   | Grants permission to modify favorites.                                                           | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>                            |
| lts:logGroup:getLogGroup | Grants permission to querying a log group.                                                       | Read         | logGroup *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:groups:get</li> </ul>                            |
| lts:IndexConfig:list     | Grants permission to querying indexes.                                                           | List         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:get</li> <li>lts:groups:get</li> </ul>    |
| lts:IndexConfig:create   | Grants permission to creating an Index.                                                          | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:put</li> <li>lts:groups:create</li> </ul> |

| Action                             | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                   | Alias                                                                      |
|------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| lts:structConfig:listStructConfig  | Grants permission to obtaining structured log stream information. | List         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>lts:wordFrequency:get</li> </ul>    |
| lts:logStream:updateLogStream      | Grants permission to modifying a log stream.                      | Write        | logStream *<br>-            | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>           |
| lts:logStream:getRealtimeLog       | Grants permission to obtaining real-time logs.                    | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>lts:logs:list</li> </ul>            |
| lts:logStream:createLogFilterRules | Grants permission to creating a log cleaning rule.                | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>        |
| lts:logStream:updateLogFilterRules | Grants permission to modifying a log cleaning rule.               | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>           |
| lts:logStream:deleteLogFilterRules | Grants permission to deleting a log cleaning rule.                | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>        |
| lts:logStream:listLogFilterRules   | Grants permission to querying log cleaning rules.                 | List         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>        |
| lts:logStream:getQuickQuery        | Grants permission to view quick queries.                          | List         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                   | <ul style="list-style-type: none"> <li>lts:searchcriterias:list</li> </ul> |

| Action                                | Description                                                       | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                    |
|---------------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|--------------------------------------------------------------------------|
| lts:logStream:updateQuickQuery        | Grants permission to modify quick query.                          | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:searchcriteria:put</li> </ul> |
| lts:logStream:searchLogContext        | Grants permission to querying the log context.                    | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:logs:list</li> </ul>          |
| lts:structConfig:getCustomTemplate    | Grants permission to querying a user-defined template.            | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>         |
| lts:structConfig:createCustomTemplate | Grants permission to creating a user-defined template.            | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>      |
| lts:structConfig:updateCustomTemplate | Grants permission to modifying a user-defined template.           | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>         |
| lts:structConfig:deleteCustomTemplate | Grants permission to deleting a user-defined template.            | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>      |
| lts:structConfig:listCustomTemplate   | Grants permission to querying the user-defined template list.     | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>         |
| lts:structConfig:smartExtra           | Grants permission to intelligent extraction of structured fields. | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>      |



| Action                                  | Description                                                                 | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                               |
|-----------------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|---------------------------------------------------------------------|
| lts:logStream: getAggrResult            | Grants permission to obtaining quick analysis results.                      | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>    |
| lts:logStream: getAggr                  | Grants permission to query quick analysis aggregator.                       | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>    |
| lts:logStream: createAggr               | Grants permission to creating a quick analysis aggregator.                  | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul> |
| lts:logStream: deleteAggr               | Grants permission to delete quick analysis aggregator.                      | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul> |
| lts:logStream: getQuickAnalysisAggValue | Grants permission to obtains the quick analysis result of the numeric type. | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -                                                                   |
| lts:logStream: getWordFreqConfig        | Grants permission to querying quick analysis fields created by users.       | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:wordFreq:get</li> </ul>  |
| lts:logStream: refreshWordFreqConfig    | Grants permission to modifying a quick analysis field.                      | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:wordFreq:set</li> </ul>  |

| Action                    | Description                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                |
|---------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------------|
| lts:logCrux:list          | Grants permission to querying log clustering information.           | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:logreduce:list</li> </ul> |
| lts:logCrux:get           | Grants permission to obtains the log clustering switch information. | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:logreduce:get</li> </ul>  |
| lts:logCrux:enable        | Grants permission to enabling Log Clustering.                       | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:logreduce:put</li> </ul>  |
| lts:logCrux:disable       | Grants permission to disabling log clustering.                      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:logreduce:put</li> </ul>  |
| lts:logStream:updateChart | Grants permission to updating the user log dashboard.               | Write        | logStream *                 | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>     |
| lts:logStream:createChart | Grants permission to creating a user log dashboard.                 | Write        | logStream *                 | -             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>  |
| lts:logStream:deleteChart | Grants permission to deleting a user log dashboard.                 | Write        | logStream *                 | -             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>  |
| lts:logStream:getChart    | Grants permission to obtaining the user log dashboard.              | Read         | logStream *                 | -             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>     |

| Action                                   | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                                                               |
|------------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------|
| lts:dashboard:deleteChart                | Grants permission to delete chart.                            | Write        | dashboard *                 | -             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul> |
| lts:dashboard:listCharts                 | Grants permission to displays charts at the dashboard level.. | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>    |
| lts:dashboard:updateChart                | Grants permission to moving charts.                           | Write        | dashboard *                 | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>    |
| lts:dashboard:getDashboard               | Grants permission to querying user log dashboards.            | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>    |
| lts:dashboardGroup:getDashboardsGroup    | Grants permission to querying user log dashboard groups.      | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>    |
| lts:dashboardGroup:updateDashboardsGroup | Grants permission to modifying a user log dashboard group.    | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>    |
| lts:dashboardGroup:deleteDashboardsGroup | Grants permission to updating user log dashboard groups.      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul> |

| Action                                              | Description                                                                              | Access Level | Resource Type (*: required) | Condition Key | Alias                                                               |
|-----------------------------------------------------|------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------|
| lts:dashboard:CreateDashboard                       | Grants permission to creating dashboards in batches based on the log dashboard template. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul> |
| lts:dashboard:CreateDashboardTemplate               | Grants permission to creating a user log dashboard template.                             | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul> |
| lts:dashboard:getDashboardTemplate                  | Grants permission to querying a user log dashboard template.                             | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>    |
| lts:dashboard:updateDashboardTemplate               | Grants permission to modifying a user log dashboard template.                            | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>    |
| lts:dashboard:deleteDashboardTemplate               | Grants permission to deleting a user log dashboard template.                             | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul> |
| lts:dashboard:Group:createLogDashboardTemplateGroup | Grants permission to creating a dashboard template group.                                | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul> |

| Action                                             | Description                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                   |
|----------------------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------------------------------------------|
| lts:dashboardGroup:updateLogDashboardTemplateGroup | Grants permission to modifying a dashboard template group.         | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>        |
| lts:dashboardGroup:deleteLogDashboardTemplateGroup | Grants permission to deleting a user log dashboard template group. | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>     |
| lts:dashboard:listFilter                           | Grants permission to querying dashboard filters.                   | List         | dashboard *                 | -             | -                                                                       |
| lts:dashboard:createFilter                         | Grants permission to Creating a Dashboard Filter.                  | Write        | dashboard *                 | -             | -                                                                       |
| lts:dashboard:updateFilter                         | Grants permission to modifying a Dashboard Filter.                 | Write        | dashboard *                 | -             | -                                                                       |
| lts:dashboard:deleteFilter                         | Grants permission to deleting a Dashboard Filter.                  | Write        | dashboard *                 | -             | -                                                                       |
| lts:alarmRule:listAlarmRules                       | Grants permission to querying the alarm rule list.                 | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul> |

| Action                             | Description                                                                                                                               | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                        |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|------------------------------------------------------------------------------|
| lts:alarmRule:getKeywordsAlarmRule | Grants permission to querying keyword alarm rules.                                                                                        | Read         | alarm Rule *                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul>      |
| lts:alarmRule:getSqlAlarmRule      | Grants permission to querying sql alarm rules.                                                                                            | Read         | alarm Rule *                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:sqlalarmrules:get</li> </ul>      |
| lts:alarm:listAlarmStatistic       | Grants permission to querying sql alarm data.                                                                                             | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:sqlalarmstatistics:get</li> </ul> |
| lts:dashboard:update               | Grants permission to modifying a user log dashboard.                                                                                      | Write        | dashboard *                 | -                                             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>             |
| lts:dashboard:delete               | Grants permission to deleting a user log dashboard.                                                                                       | Write        | dashboard *                 | -                                             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>          |
| lts:logSearch:list                 | Grants permission to obtains the cluster list, namespace, component, instance, log, node, and log file page component list and file list. | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>               |

| Action                                   | Description                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                                                               |
|------------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------|
| lts:logSearch:getTime                    | Grants permission to obtains the current time of the backend node. | Read         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:get</li> </ul>       |
| lts:supportCloudService:listCloudService | Grants permission to list supported cloud services.                | Read         | -                           | -             | -                                                                   |
| lts:logSearch:getLogContext              | Grants permission to obtaining the log context.                    | Read         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:get</li> </ul>       |
| lts:logSearch:exportLogs                 | Grants permission to download logs.                                | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>      |
| lts:ageingTime:get                       | Grants permission to obtaining quota management.                   | List         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>      |
| lts:ageingTime:update                    | Grants permission to modify quota management.                      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:quota:set</li> </ul>     |
| lts:logConfigPath:list                   | Grants permission to querying the vm log path configuration.       | List         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>      |
| lts:logConfigPath:create                 | Grants permission to configuring the log path of a new vm.         | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |

| Action                | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias                                                               |
|-----------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------|
| lts:structRule:get    | Grants permission to obtaining structured rules.                                 | Read         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:get</li> </ul>       |
| lts:structRule:create | Grants permission to creating a structured rule.                                 | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:structRule:delete | Grants permission to deleting a structured rule.                                 | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:structRule:regex  | Grants permission to structured extraction.                                      | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:logPail:list      | Grants permission to querying a log bucket, logs in a bucket, and log bar chart. | List         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>      |
| lts:structSql:list    | Grants permission to querying structured logs.                                   | List         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>      |
| lts:logPail:create    | Grants permission to adding a log bucket.                                        | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:logPail:update    | Grants permission to modifying a log bucket.                                     | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |



| Action                     | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                                               |
|----------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------|
| lts:logPail:delete         | Grants permission to deleting a log bucket.                                | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:storageRelation:list   | Grants permission to querying the dump relationship of the current tenant. | List         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>      |
| lts:storageRelation:delete | Grants permission to delete the dump relationship of the current tenant.   | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:storage:batchAction    | Grants permission to periodic batch start and stop.                        | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:logPailDump:create     | Grants permission to add log dump.                                         | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:statisticsRule:list    | Grants permission to querying statistics rules.                            | List         | -                           | -             | <ul style="list-style-type: none"> <li>aom:log:list</li> </ul>      |
| lts:statisticsRule:create  | Grants permission to creating a statistics rule.                           | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:statisticsRule:update  | Grants permission to modifying a statistics rule.                          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |

| Action                              | Description                                              | Access Level | Resource Type (*: required) | Condition Key | Alias                                                               |
|-------------------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------|
| lts:statisticsRule:delete           | Grants permission to deleting a statistical rule.        | Write        | -                           | -             | <ul style="list-style-type: none"> <li>aom:subscribe:set</li> </ul> |
| lts:transfer:listKafkaInstanceTopic | Grants permission to obtains all Kafka topics of a user. | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:kafka:list</li> </ul>    |
| lts:logPackage:create               | Grants permission to purchase a resource package.        | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>    |
| lts:consumerGroup:create            | Grants permission to creating a consumer group.          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul> |
| lts:consumerGroup:delete            | Grants permission to deleting a consumer group.          | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul> |
| lts:consumerGroup:list              | Grants permission to querying the consumer group list.   | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:list</li> </ul>   |
| lts:consumerGroup:get               | Grants permission to querying consumer group details.    | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>    |
| lts:consumerGroup:update            | Grants permission to modify consumer group.              | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:topics:put</li> </ul>    |

| Action                        | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                    |
|-------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|--------------------------------------------------------------------------|
| lts:logStream:get             | Grants permission to obtaining log flow details.                                    | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>         |
| lts:agency:listGroupAndStream | Grants permission to obtains the log stream list of the log group of the delegator. | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>         |
| lts:agency:listEps            | Grants permission to obtain the eps list of the entrusting party.                   | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>         |
| lts:agency:listStructConfig   | Grants permission to obtaining the structured configuration of the delegator.       | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>         |
| lts:logConverge:get           | Grants permission to obtaining Multi-Account log aggregation configuration.         | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:logConverge:get</li> </ul>    |
| lts:logConverge:update        | Grants permission to update Multi-Account log aggregation configuration.            | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:logConverge:update</li> </ul> |

| Action                          | Description                                                  | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                                            |
|---------------------------------|--------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|--------------------------------------------------------------------------------------------------|
| lts:logManager:createAggr       | Grants permission to create a quick analysis aggregator.     | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>                              |
| lts:logManager:createAggrs      | Grants permission to create some quick analysis aggregators. | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:create</li> </ul>                              |
| lts:logManager:deleteAggr       | Grants permission to delete the Quick Analysis Aggregator.   | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>                              |
| lts:logManager:deleteAggrs      | Grants permission to bulk delete Quick Analysis Aggregators. | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:topics:delete</li> </ul>                              |
| lts:logManager:createLogFilter  | Grants permission to create log filter rules.                | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:filters:create</li> </ul>                             |
| lts:logManager:listLogFilters   | Grants permission to view log filter rules.                  | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:filters:list</li> </ul>                               |
| lts:logManager:updateLogFilters | Grants permission to modify log filter rules.                | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:filters:put</li> <li>lts:filtersAction:put</li> </ul> |
| lts:logManager:deleteLogFilters | Grants permission to delete log filter rules.                | Write        | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:filters:delete</li> </ul>                             |

| Action                                 | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                      |
|----------------------------------------|----------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------------------------------------------------|
| lts:structConfig:regex                 | Grants permission to regularize structuring sample logs. | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:regex:create</li> </ul>         |
| lts:structConfig:listAllCustomTemplate | Grants permission to list all custom templates.          | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>           |
| lts:tag:get                            | Grants permission to get tag.                            | Read         | logGroup                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | <ul style="list-style-type: none"> <li>lts:resourceTags:get</li> </ul>     |
|                                        |                                                          |              | logStream                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                                                            |
|                                        |                                                          |              | accessConfig                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                                                            |
|                                        |                                                          |              | hostGroup                   | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                                                            |
| lts:tag:list                           | Grants permission to list tag.                           | List         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:topics:get</li> </ul>           |
| lts:subscription:create                | Grants permission to create subscription info.           | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:subscriptions:create</li> </ul> |
| lts:subscription:get                   | Grants permission to get subscription info.              | Read         | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:subscriptions:get</li> </ul>    |
| lts:subscription:update                | Grants permission to update subscription info.           | Write        | -                           | -                                             | <ul style="list-style-type: none"> <li>lts:subscriptions:put</li> </ul>    |

| Action                             | Description                                         | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias                                                                       |
|------------------------------------|-----------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| lts:subscription:delete            | Grants permission to delete subscription info.      | Write        | -                           | -                                                                                                                                 | <ul style="list-style-type: none"> <li>lts:subscriptions:delete</li> </ul>  |
| lts:logStream:getSqlAnalysisResult | Grants permission to get SQL query analysis result. | Read         | logStream *                 | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -                                                                           |
| lts:resource:listResourcesByTags   | Grants permission to get resource instance list.    | List         | logGroup                    | -                                                                                                                                 | <ul style="list-style-type: none"> <li>lts:resourceInstance:list</li> </ul> |
|                                    |                                                     |              | logStream                   | -                                                                                                                                 |                                                                             |
|                                    |                                                     |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |                                                                             |
| lts:log2MetricRule:create          | Grants permission to create log-to-metric rule.     | Write        | -                           | -                                                                                                                                 | -                                                                           |
| lts:log2MetricRule:update          | Grants permission to update log-to-metric rule.     | Write        | -                           | -                                                                                                                                 | -                                                                           |
| lts:log2MetricRule:delete          | Grants permission to delete log-to-metric rule.     | Write        | -                           | -                                                                                                                                 | -                                                                           |
| lts:log2MetricRule:list            | Grants permission to get log-to-metric rule list.   | List         | -                           | -                                                                                                                                 | -                                                                           |

| Action                 | Description                                           | Access Level | Resource Type (*: required) | Condition Key | Alias                                                          |
|------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------------------------------|
| lts:log2MetricRule:get | Grants permission to get log-to-metric rule detail.   | Read         | -                           | -             | -                                                              |
| lts:streamConsume:get  | Grants permission to get stream consume details.      | Read         | -                           | -             | <ul style="list-style-type: none"><li>lts:groups:get</li></ul> |
| lts:dsl:get            | Grants permission to get log processing task details. | Read         | -                           | -             | -                                                              |
| lts:dsl:list           | Grants permission to get log processing task list.    | List         | -                           | -             | -                                                              |
| lts:dsl:create         | Grants permission to create log processing task.      | Write        | -                           | -             | -                                                              |
| lts:dsl:update         | Grants permission to update log processing task.      | Write        | -                           | -             | -                                                              |
| lts:dsl:delete         | Grants permission to delete log processing task.      | Write        | -                           | -             | -                                                              |

| Action                     | Description                                                             | Access Level | Resource Type (*: required) | Condition Key | Alias                                                                           |
|----------------------------|-------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------------------------------------------|
| lts:aiops:nl2ql            | Grants permission to invoke LLM for natural language conversion to SQL. | Read         | -                           | -             | -                                                                               |
| lts::listAgentConf         | Grants permission to query agent collection configuration.              | List         | -                           | -             | <ul style="list-style-type: none"> <li>lts:agentsConf:list</li> </ul>           |
| lts::getEipReportEnable    | Grants permission to access public network report logs.                 | Read         | -                           | -             | <ul style="list-style-type: none"> <li>lts:log:getEipReportEnable</li> </ul>    |
| lts::updateEipReportEnable | Grants permission to update public network report logs.                 | Write        | -                           | -             | <ul style="list-style-type: none"> <li>lts:log:updateEipReportEnable</li> </ul> |

Each API of LTS usually supports one or more actions. [Table 3-272](#) lists the supported actions and dependencies.

**Table 3-272** Actions and dependencies supported by LTS APIs

| API                                           | Action                      | Dependencies |
|-----------------------------------------------|-----------------------------|--------------|
| POST /v2/{project_id}/groups                  | lts:logGroup:createLogGroup | -            |
| DELETE /v2/{project_id}/groups/{log_group_id} | lts:logGroup:deleteLogGroup | -            |
| GET /v2/{project_id}/groups                   | lts:logGroup:listLogGroup   | -            |



| API                                                                                      | Action                           | Dependencies |
|------------------------------------------------------------------------------------------|----------------------------------|--------------|
| POST /v2/{project_id}/groups/{log_group_id}                                              | lts:logGroup:updateLogGroup      | -            |
| POST /v2/{project_id}/groups/{log_group_id}/streams                                      | lts:logStream:createLogStream    | -            |
| PUT /v2/{project_id}/groups/{log_group_id}/streams-ttl/{log_stream_id}                   | lts:logStream:updateLogStream    | -            |
| DELETE /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}                    | lts:logStream:deleteLogStream    | -            |
| GET /v2/{project_id}/groups/{log_group_id}/streams                                       | lts:logStream:listLogStream      | -            |
| GET /v2/{project_id}/log-streams                                                         | lts:logStream:listLogStream      | -            |
| POST /v2/{project_id}/lts/keyword-count                                                  | lts:logStream:searchLogHistogram | -            |
| POST /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/content/query        | lts:logStream:searchLog          | -            |
| POST /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/struct-content/query | lts:logStream:searchStructLog    | -            |

| API                                                                | Action                                   | Dependencies                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v2/{project_id}/streams/{log_stream_id}/struct-content/query | lts:logStream:searchStructLog            | -                                                                                                                                                                                                                                                               |
| POST /v2/{project_id}/transfers                                    | lts:transfer:createTransfer              | <ul style="list-style-type: none"> <li>• obs:bucket:PutBucketAcl</li> <li>• obs:bucket:GetBucketAcl</li> <li>• obs:bucket:GetEncryptionConfiguration</li> <li>• obs:bucket:HeadBucket</li> <li>• dis:streams:list</li> <li>• dis:streamPolicies:list</li> </ul> |
| DELETE /v2/{project_id}/transfers                                  | lts:transfer:deleteTransfer              | -                                                                                                                                                                                                                                                               |
| GET /v2/{project_id}/transfers                                     | lts:transfer:listTransfer                | -                                                                                                                                                                                                                                                               |
| POST /v2/{project_id}/lts/dms/kafka-instance                       | lts:transfer:registerDmsKafkaInstance    | dms:instance:list                                                                                                                                                                                                                                               |
| PUT /v2/{project_id}/transfers                                     | lts:transfer:updateTransfer              | <ul style="list-style-type: none"> <li>• obs:bucket:PutBucketAcl</li> <li>• obs:bucket:GetBucketAcl</li> <li>• obs:bucket:GetEncryptionConfiguration</li> <li>• obs:bucket:HeadBucket</li> <li>• dis:streams:list</li> <li>• dis:streamPolicies:list</li> </ul> |
| POST /v2/{project_id}/collection/disable                           | lts:configCenter:updateOverCollectSwitch | -                                                                                                                                                                                                                                                               |
| POST /v2/{project_id}/collection/enable                            | lts:configCenter:updateOverCollectSwitch | -                                                                                                                                                                                                                                                               |
| POST /v3/{project_id}/lts/struct/template                          | lts:structConfig:createStructConfig      | -                                                                                                                                                                                                                                                               |
| DELETE /v2/{project_id}/lts/struct/template                        | lts:structConfig:deleteStructConfig      | -                                                                                                                                                                                                                                                               |

| API                                                                   | Action                              | Dependencies   |
|-----------------------------------------------------------------------|-------------------------------------|----------------|
| GET /v3/{project_id}/lts/struct/customtemplate/list                   | lts:structConfig:listStructTemplate | -              |
| GET /v3/{project_id}/lts/struct/customtemplate                        | lts:structConfig:listStructTemplate | -              |
| GET /v2/{project_id}/lts/struct/template                              | lts:structConfig:getStructConfig    | -              |
| PUT /v3/{project_id}/lts/struct/template                              | lts:structConfig:updateStructConfig | -              |
| POST /v2/{project_id}/lts/aom-mapping                                 | lts:mappingRule:create              | -              |
| DELETE /v2/{project_id}/lts/aom-mapping                               | lts:mappingRule:delete              | -              |
| GET /v2/{project_id}/lts/aom-mapping/{rule_id}                        | lts:mappingRule:get                 | -              |
| GET /v2/{project_id}/lts/aom-mapping                                  | lts:mappingRule:list                | -              |
| PUT /v2/{project_id}/lts/aom-mapping                                  | lts:mappingRule:update              | -              |
| GET /v2/{project_id}/lts/notifications/topics                         | lts:alarmNoticeTemplate:list        | smn:topic:list |
| POST /v2/{project_id}/lts/alarms/sql-alarm-rule                       | lts:alarmRule:createSqlAlarmRule    | -              |
| DELETE /v2/{project_id}/lts/alarms/sql-alarm-rule/{sql_alarm_rule_id} | lts:alarmRule:deleteSqlAlarmRule    | -              |

| API                                                                             | Action                            | Dependencies |
|---------------------------------------------------------------------------------|-----------------------------------|--------------|
| GET /v2/{project_id}/lts/alarms/sql-alarm-rule                                  | lts:alarmRule:listSqlAlarmRule    | -            |
| PUT /v2/{project_id}/lts/alarms/status                                          | lts:alarmRule:updateSqlAlarmRule  | -            |
| PUT /v2/{project_id}/lts/alarms/sql-alarm-rule                                  | lts:alarmRule:updateSqlAlarmRule  | -            |
| POST /v2/{project_id}/lts/alarms/keywords-alarm-rule                            | lts:alarmRule:createWordAlarmRule | -            |
| DELETE /v2/{project_id}/lts/alarms/keywords-alarm-rule/{keywords_alarm_rule_id} | lts:alarmRule:deleteWordAlarmRule | -            |
| GET /v2/{project_id}/lts/alarms/keywords-alarm-rule                             | lts:alarmRule:listWordAlarmRule   | -            |
| PUT /v2/{project_id}/lts/alarms/keywords-alarm-rule                             | lts:alarmRule:updateWordAlarmRule | -            |
| POST /v2/{project_id}/{domain_id}/lts/alarms/sql-alarm/clear                    | lts:alarm:cleanAlarm              | -            |
| POST /v2/{project_id}/{domain_id}/lts/alarms/sql-alarm/query                    | lts:alarm:listAlarm               | -            |

| API                                                                               | Action                         | Dependencies |
|-----------------------------------------------------------------------------------|--------------------------------|--------------|
| GET /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/charts         | lts:logStream:listChart        | -            |
| POST /v2/{project_id}/{domain_id}/lts/events/notification/templates               | lts:alarmNoticeTemplate:create | -            |
| DELETE /v2/{project_id}/{domain_id}/lts/events/notification/templates             | lts:alarmNoticeTemplate:delete | -            |
| POST /v2/{project_id}/{domain_id}/lts/events/notification/templates/view          | lts:alarmNoticeTemplate:list   | -            |
| GET /v2/{project_id}/{domain_id}/lts/events/notification/templates                | lts:alarmNoticeTemplate:list   | -            |
| GET /v2/{project_id}/{domain_id}/lts/events/notification/template/{template_name} | lts:alarmNoticeTemplate:get    | -            |
| PUT /v2/{project_id}/{domain_id}/lts/events/notification/templates                | lts:alarmNoticeTemplate:update | -            |
| POST /v3/{project_id}/lts/host-group                                              | lts:hostGroup:create           | -            |
| DELETE /v3/{project_id}/lts/host-group                                            | lts:hostGroup:delete           | -            |

| API                                                                            | Action                         | Dependencies                                                                            |
|--------------------------------------------------------------------------------|--------------------------------|-----------------------------------------------------------------------------------------|
| POST /v3/{project_id}/lts/host-list                                            | lts:host:list                  | <ul style="list-style-type: none"> <li>aom:icmgr:get</li> <li>aom:icmgr:list</li> </ul> |
| POST /v3/{project_id}/lts/host-group-list                                      | lts:hostGroup:list             | -                                                                                       |
| PUT /v3/{project_id}/lts/host-group                                            | lts:hostGroup:update           | -                                                                                       |
| POST /v3/{project_id}/lts/access-config                                        | lts:accessConfig:create        | -                                                                                       |
| DELETE /v3/{project_id}/lts/access-config                                      | lts:accessConfig:delete        | -                                                                                       |
| POST /v3/{project_id}/lts/access-config-list                                   | lts:accessConfig:list          | -                                                                                       |
| PUT /v3/{project_id}/lts/access-config                                         | lts:accessConfig:update        | -                                                                                       |
| POST /v1/{project_id}/{resource_type}/{resource_id}/tags/action                | lts:tag:create                 | -                                                                                       |
| POST /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias   | lts:logStream:createQuickQuery | -                                                                                       |
| DELETE /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias | lts:logStream:deleteQuickQuery | -                                                                                       |
| GET /v1.0/{project_id}/groups/{group_id}/topics/{topic_id}/search-criterias    | lts:logStream:listQuickQuery   | -                                                                                       |

| API                                                                         | Action                         | Dependencies |
|-----------------------------------------------------------------------------|--------------------------------|--------------|
| GET /v2/{project_id}/lts/history-sql                                        | lts:logStream:getHistorySql    | -            |
| GET /v1.0/{project_id}/lts/groups/{group_id}/search-criterias               | lts:logStream:listQuickQuery   | -            |
| POST /v1.0/{project_id}/lts/favorite                                        | lts:logFavorite:create         | -            |
| DELETE /v1.0/{project_id}/lts/favorite/{fav_res_id}                         | lts:logFavorite:delete         | -            |
| POST /v2/{project_id}/dashboard                                             | lts:dashboard:create           | -            |
| POST /v2/{project_id}/lts/dashboard-group                                   | lts:dashboardGroup:create      | -            |
| POST /v2/{project_id}/lts/timeline-traffic-statistics                       | lts:trafficStatistic:get       | -            |
| POST /v2/{project_id}/lts/topn-traffic-statistics                           | lts:trafficStatistic:get       | -            |
| POST /v1.0/{project_id}/groups/{group_id}/stream/{stream_id}/index/config   | lts:IndexConfig:create         | -            |
| GET /v1.0/{project_id}/groups/{group_id}/stream/{stream_id}/index/config    | lts:IndexConfig:list           | -            |
| POST /v2/{project_id}/groups/{log_group_id}/streams/{log_stream_id}/context | lts:logStream:searchLogContext | -            |

| API                                                              | Action                  | Dependencies |
|------------------------------------------------------------------|-------------------------|--------------|
| POST /v2.0/{project_id}/lts/createAgencyAccess                   | lts:accessConfig:create | -            |
| GET /v1/{project_id}/lts/{member_account_id}/all-streams         | lts:logConverge:get     | -            |
| GET /v1/{project_id}/lts/log-converge-config/{member_account_id} | lts:logConverge:get     | -            |
| PUT /v1/{project_id}/lts/log-converge-config/switch              | lts:logConverge:update  | -            |
| PUT /v1/{project_id}/lts/log-converge-config                     | lts:logConverge:update  | -            |
| GET /v1/{project_id}/lts/log-converge-config/switch              | lts:logConverge:get     | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-273](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for LTS.

**Table 3-273** Resource types supported by LTS

| Resource Type | URN                                                        |
|---------------|------------------------------------------------------------|
| logStream     | lts:<region>:<account-id>:logStream:<group_id>/<stream_id> |
| logGroup      | lts:<region>:<account-id>:logGroup:<group_id>              |



| Resource Type | URN                                                 |
|---------------|-----------------------------------------------------|
| dashboard     | lts:<region>:<account-id>:dashboard:<dashboard_id>  |
| accessConfig  | lts:<region>:<account-id>:accessConfig:<config_id>  |
| alarmRule     | lts:<region>:<account-id>:alarmRule:<alarm_rule_id> |
| transfer      | lts:<region>:<account-id>:transfer:<transfer_id>    |
| hostGroup     | lts:<region>:<account-id>:hostGroup:<host_group_id> |

## Conditions

LTS does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.14.11 Actions Supported by Identity Policy-based Authorization

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.

- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by cts, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by cts, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for cts.

**Table 3-274** Actions supported by cts

| Action             | Description                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------|---------------------------------------|--------------|-----------------------------|---------------|-------|
| cts:trace:list     | Grants permission to query cts trace. | List         | -                           | -             | -     |
| cts:tracker:create | Grants permission to create tracker.  | Write        | -                           | -             | -     |
| cts:tracker:list   | Grants permission to list trackers.   | List         | -                           | -             | -     |

| Action                  | Description                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|-------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| cts:tracker:update      | Grants permission to update tracker.                      | Write        | tracker                     | -                                                                                                                                     | -     |
| cts:tracker:delete      | Grants permission to delete an tracker.                   | Write        | tracker                     | -                                                                                                                                     | -     |
| cts:quota:get           | Grants permission to query the tracker quota of a tenant. | Read         | -                           | -                                                                                                                                     | -     |
| cts:notification:create | Grants permission to create notification.                 | Write        | -                           | -                                                                                                                                     | -     |
| cts:notification:update | Grants permission to update notification.                 | Write        | notification                | -                                                                                                                                     | -     |
| cts:notification:list   | Grants permission to list notifications.                  | List         | -                           | -                                                                                                                                     | -     |
| cts:notification:delete | Grants permission to delete the notification.             | Write        | notification                | -                                                                                                                                     | -     |
| cts:tag:create          | Grants permission to create the resource tags.            | Tagging      | tracker                     | -                                                                                                                                     | -     |
|                         |                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> |       |
| cts:tag:delete          | Grants permission to delete the tracker tags.             | Tagging      | tracker                     | -                                                                                                                                     | -     |

| Action                         | Description                                              | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias |
|--------------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                |                                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> |       |
| cts:notification:listOperation | Grants permission to query all operation list.           | List         | -                           | -                                                                                                                                     | -     |
| cts:trace:listTraceUser        | Grants permission to query all user list.                | List         | -                           | -                                                                                                                                     | -     |
| cts:trace:listResource         | Grants permission to query all trace resource type list. | List         | -                           | -                                                                                                                                     | -     |

Each API of cts usually supports one or more actions. [Table 3-275](#) lists the supported actions and dependencies.

**Table 3-275** Actions and dependencies supported by cts APIs

| API                         | Action         | Dependencies |
|-----------------------------|----------------|--------------|
| GET /v3/{project_id}/traces | cts:trace:list | -            |
| GET /v3/{project_id}/quotas | cts:quota:get  | -            |

| API                                   | Action                  | Dependencies                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v3/{project_id}/tracker         | cts:tracker:create      | <ul style="list-style-type: none"> <li>• lts:topics:list</li> <li>• lts:topics:create</li> <li>• lts:groups:list</li> <li>• lts:groups:create</li> <li>• obs:bucket:CreateBucket</li> <li>• obs:bucket:HeadBucket</li> <li>• obs:bucket:GetLifecycleConfiguration</li> <li>• obs:bucket:PutLifecycleConfiguration</li> <li>• obs:bucket:GetBucketAcl</li> <li>• obs:bucket:PutBucketAcl</li> <li>• kms:cmk:list</li> </ul> |
| PUT /v3/{project_id}/tracker          | cts:tracker:update      | <ul style="list-style-type: none"> <li>• lts:topics:list</li> <li>• lts:topics:create</li> <li>• lts:groups:list</li> <li>• lts:groups:create</li> <li>• obs:bucket:CreateBucket</li> <li>• obs:bucket:HeadBucket</li> <li>• obs:bucket:GetLifecycleConfiguration</li> <li>• obs:bucket:PutLifecycleConfiguration</li> <li>• obs:bucket:GetBucketAcl</li> <li>• obs:bucket:PutBucketAcl</li> <li>• kms:cmk:list</li> </ul> |
| GET /v3/{project_id}/trackers         | cts:tracker:list        | -                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DELETE /v3/{project_id}/trackers      | cts:tracker:delete      | -                                                                                                                                                                                                                                                                                                                                                                                                                          |
| POST /v3/{project_id}/notifications   | cts:notification:create | <ul style="list-style-type: none"> <li>• smn:topic:listTopic</li> <li>• iam:users:listUsers</li> <li>• iam:groups:listGroups</li> </ul>                                                                                                                                                                                                                                                                                    |
| PUT /v3/{project_id}/notifications    | cts:notification:update | <ul style="list-style-type: none"> <li>• smn:topic:listTopic</li> <li>• iam:users:listUsers</li> <li>• iam:groups:listGroups</li> </ul>                                                                                                                                                                                                                                                                                    |
| DELETE /v3/{project_id}/notifications | cts:notification:delete | -                                                                                                                                                                                                                                                                                                                                                                                                                          |

| API                                                               | Action                         | Dependencies                |
|-------------------------------------------------------------------|--------------------------------|-----------------------------|
| GET /v3/{project_id}/notifications/{notification_type}            | cts:notification:list          | -                           |
| POST /v3/{project_id}/{resource_type}/{resource_id}/tags/create   | cts:tag:create                 | -                           |
| DELETE /v3/{project_id}/{resource_type}/{resource_id}/tags/delete | cts:tag:delete                 | -                           |
| GET /v3/{domain_id}/resources                                     | cts:trace:listResource         | -                           |
| GET /v3/{project_id}/operations                                   | cts:notification:listOperation | -                           |
| GET /v3/{project_id}/user-resources                               | cts:trace:listTraceUser        | -                           |
| POST /v3/{domain_id}/checkbucket                                  | cts:tracker:list               | obs:bucket:ListAllMyBuckets |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-276](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for cts.

**Table 3-276** Resource types supported by cts

| Resource Type | URN                                            |
|---------------|------------------------------------------------|
| tracker       | cts:<region>:<account-id>:tracker:<tracker-id> |

| Resource Type | URN                                                      |
|---------------|----------------------------------------------------------|
| notification  | cts:<region>:<account-id>:notification:<notification-id> |

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **cts:**) only apply to operations of the BMS service. For details, see [Table 3-277](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so **g:SourceVpce** is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so **g:TagKeys** is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Condition operators](#).

The following table lists the condition keys that you can define in SCPs for CTS. You can include these condition keys to specify conditions for when your SCP is in effect.

**Table 3-277** Service-specific condition keys supported by CTS

| Condition Key  | Type   | Single-valued/<br>Multivalued | Description                                  |
|----------------|--------|-------------------------------|----------------------------------------------|
| cts:TargetType | string | Single-valued                 | Filter access permissions by data dump type. |

| Condition Key       | Type   | Single-valued/<br>Multivalued | Description                                                                                                |
|---------------------|--------|-------------------------------|------------------------------------------------------------------------------------------------------------|
| cts:TargetAccountId | string | Single-valued                 | Filter access permissions based on the domain ID (account ID) of the user to which the OBS bucket belongs. |
| cts:TargetOrgId     | string | Single-valued                 | Filter access permissions based on the organization to which the OBS bucket belongs.                       |
| cts:TargetOrgPath   | string | Single-valued                 | Filter access permissions based on the OU path of the organization to which the OBS bucket belongs.        |

### 3.14.12 Resource Formation Service (RFS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).



## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by STS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by STS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for IAC.

**Table 3-278** Actions supported by IAC

| Action                  | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rf:privateTemplate:list | Grants permission to obtain private template list of project. | list         | privateTemplate*            | -             | -     |

| Action                                | Description                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rf:privateTemplate:create             | Grants permission to create a private template.                       | write        | privateTemplate*            | -             | -     |
| rf:privateTemplate:delete             | Grants permission to delete a private template.                       | write        | privateTemplate*            | -             | -     |
| rf:privateTemplate:showMetadata       | Grants permission to display the details of private template.         | read         | privateTemplate*            | -             | -     |
| rf:privateTemplate:updateMetadata     | Grants permission to update the metadata of private template.         | write        | privateTemplate*            | -             | -     |
| rf:privateTemplate:listVersions       | Grants permission to display all version details of private template. | list         | privateTemplate*            | -             | -     |
| rf:privateTemplate:createVersion      | Grants permission to create a private template version.               | write        | privateTemplate*            | -             | -     |
| rf:privateTemplate:showVersionContent | Grants permission to obtain the content of private template version.  | read         | privateTemplate*            | -             | -     |

| Action                                 | Description                                                        | Access Level | Resource Type (*: required) | Condition Key | Alias                     |
|----------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------|
| rf:privateTemplate:deleteVersion       | Grants permission to delete a private template version.            | write        | privateTemplate*            | -             | -                         |
| rf:privateTemplate:showVersionMetadata | Grants permission to get the metadata of private template version. | read         | privateTemplate*            | -             | -                         |
| rf:stack:create                        | Grants permission to create a stack.                               | write        | stack*                      | -             | rf:stack:createStack      |
| rf:stack:deploy                        | Grants permission to deploy a stack.                               | write        | stack*                      | -             | rf:stack:deployStack      |
| rf:stack:list                          | Grants permission to list all stacks.                              | list         | stack*                      | -             | rf:stack:listStacks       |
| rf:stack:getMetadata                   | Grants permission to get the metadata of a stack.                  | read         | stack*                      | -             | rf:stack:getStackMetadata |
| rf:stack:delete                        | Grants permission to delete a stack.                               | write        | stack*                      | -             | rf:stack:deleteStack      |
| rf:stack:getTemplate                   | Grants permission to get the template of a stack.                  | read         | stack*                      | -             | rf:stack:getStackTemplate |

| Action                            | Description                                                 | Access Level | Resource Type (*: required) | Condition Key | Alias                       |
|-----------------------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------|
| rf:stack:listEvents               | Grants permission to list deployment events of a stack.     | list         | stack *                     | -             | rf:stack:listStackEvents    |
| rf:stack:listResources            | Grants permission to list all resources of a stack.         | list         | stack *                     | -             | rf:stack:listStackResources |
| rf:stack:listOutputs              | Grants permission to list all outputs of a stack.           | list         | stack *                     | -             | rf:stack:listStackOutputs   |
| rf:stack:createExecutionPlan      | Grants permission to create an execution plan.              | write        | stack *                     | -             | -                           |
| rf:stack:getExecutionPlanMetadata | Grants permission to get the metadata of an execution plan. | read         | stack *                     | -             | -                           |
| rf:stack:getExecutionPlan         | Grants permission to get an execution plan.                 | read         | stack *                     | -             | -                           |
| rf:stack:applyExecutionPlan       | Grants permission to apply an execution plan.               | write        | stack *                     | -             | -                           |
| rf:stack:listExecutionPlans       | Grants permission to list all execution plans.              | list         | stack *                     | -             | -                           |

| Action                              | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias                          |
|-------------------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------|
| rf:stack:deleteExecutionPlan        | Grants permission to delete an execution plan.                | write        | stack *                     | -             | -                              |
| rf:stack:continueRollback           | Grants permission to continue rolling back the stack.         | write        | stack *                     | -             | rf:stack:continueRollbackStack |
| rf:stack:continueDeploy             | Grants permission to continue to deploy the stack.            | write        | stack *                     | -             | rf:stack:continueDeployStack   |
| rf:stack:estimateExecutionPlanPrice | Grants permission to estimate the price of an execution plan. | read         | stack *                     | -             | -                              |
| rf:stack:update                     | Grants permission to update stack properties.                 | write        | stack *                     | -             | rf:stack:updateStack           |
| rf:stackSet:create                  | Grants permission to create a stack set.                      | write        | stack Set *                 | -             | -                              |
| rf:stackSet:list                    | Grants permission to list all stack sets.                     | list         | stack Set *                 | -             | -                              |
| rf:stackSet:showTemplate            | Grants permission to show the template of a stack set.        | read         | stack Set *                 | -             | -                              |

| Action                            | Description                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rf:stackSet:showMetadata          | Grants permission to show the metadata of a stack set.            | read         | stack Set *                 | -             | -     |
| rf:stackSet:deploy                | Grants permission to deploy a stack set.                          | write        | stack Set *                 | -             | -     |
| rf:stackSet:delete                | Grants permission to delete a stack set.                          | write        | stack Set *                 | -             | -     |
| rf:stackSet:update                | Grants permission to update stack set properties.                 | write        | stack Set *                 | -             | -     |
| rf:stackSet:listStackInstances    | Grants permission to list all stack instances.                    | list         | stack Set *                 | -             | -     |
| rf:stackSet:createStackInstances  | Grants permission to create stack instances.                      | write        | stack Set *                 | -             | -     |
| rf:stackSet:deleteStackInstances  | Grants permission to delete stack instances.                      | write        | stack Set *                 | -             | -     |
| rf:stackSet:showOperationMetadata | Grants permission to show the metadata of an stack set operation. | read         | stack Set *                 | -             | -     |
| rf:stackSet:listOperations        | Grants permission to list all stack set operations.               | list         | stack Set *                 | -             | -     |

Each API of IAC usually supports one or more actions. [Table 3-279](#) lists the supported actions and dependencies.

**Table 3-279** Actions and dependencies supported by IAC APIs

| API                                                                  | Action                                | Dependencies |
|----------------------------------------------------------------------|---------------------------------------|--------------|
| GET /v1/{project_id}/templates                                       | rf:privateTemplate:list               | -            |
| POST /v1/{project_id}/templates                                      | rf:privateTemplate:create             | -            |
| DELETE /v1/{project_id}/templates/{template_name}                    | rf:privateTemplate:delete             | -            |
| GET /v1/{project_id}/templates/{template_name}/metadata              | rf:privateTemplate:showMetadata       | -            |
| PATCH /v1/{project_id}/templates/{template_name}/metadata            | rf:privateTemplate:updateMetadata     | -            |
| GET /v1/{project_id}/templates/{template_name}/versions              | rf:privateTemplate:listVersions       | -            |
| POST /v1/{project_id}/templates/{template_name}/versions             | rf:privateTemplate:createVersion      | -            |
| GET /v1/{project_id}/templates/{template_name}/versions/{version_id} | rf:privateTemplate:showVersionContent | -            |

| API                                                                                                   | Action                                 | Dependencies                                                                                        |
|-------------------------------------------------------------------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------|
| DELETE /v1/<br>{project_id}/<br>templates/<br>{template_name}/<br>versions/<br>{version_id}           | rf:privateTemplate:deleteVersion       | -                                                                                                   |
| GET /v1/<br>{project_id}/<br>templates/<br>{template_name}/<br>versions/<br>{version_id}/<br>metadata | rf:privateTemplate:showVersionMetadata | -                                                                                                   |
| POST /v1/<br>{project_id}/stacks                                                                      | rf:stack:create                        | <ul style="list-style-type: none"> <li>kms:cmk:decryptDataKey</li> <li>iam:agencies:pass</li> </ul> |
| POST /v1/<br>{project_id}/stacks/<br>{stack_name}/<br>deployments                                     | rf:stack:deploy                        | kms:cmk:decryptDataKey                                                                              |
| GET /v1/<br>{project_id}/stacks                                                                       | rf:stack:list                          | -                                                                                                   |
| GET /v1/<br>{project_id}/stacks/<br>{stack_name}/<br>metadata                                         | rf:stack:getMetadata                   | -                                                                                                   |
| DELETE /v1/<br>{project_id}/stacks/<br>{stack_name}                                                   | rf:stack:delete                        | -                                                                                                   |
| GET /v1/<br>{project_id}/stacks/<br>{stack_name}/<br>templates                                        | rf:stack:getTemplate                   | -                                                                                                   |
| GET /v1/<br>{project_id}/stacks/<br>{stack_name}/<br>events                                           | rf:stack:listEvents                    | -                                                                                                   |
| GET /v1/<br>{project_id}/stacks/<br>{stack_name}/<br>resources                                        | rf:stack:listResources                 | -                                                                                                   |



| API                                                                                     | Action                             | Dependencies           |
|-----------------------------------------------------------------------------------------|------------------------------------|------------------------|
| GET /v1/{project_id}/stacks/{stack_name}/outputs                                        | rf:stack:listOutputs               | -                      |
| POST /v1/{project_id}/stacks/{stack_name}/execution-plans                               | rf:stack:createExecutionPlan       | kms:cmk:decryptDataKey |
| GET /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}/metadata | rf:stack:getExecutionPlan-Metadata | -                      |
| GET /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}          | rf:stack:getExecutionPlan          | -                      |
| POST /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}         | rf:stack:applyExecutionPlan        | -                      |
| GET /v1/{project_id}/stacks/{stack_name}/execution-plans                                | rf:stack:listExecutionPlans        | -                      |
| DELETE /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}       | rf:stack:deleteExecutionPlan       | -                      |
| POST /v1/{project_id}/stacks/{stack_name}/rollbacks                                     | rf:stack:continueRollback          | -                      |
| POST /v1/{project_id}/stacks/{stack_name}/continuations                                 | rf:stack:continueDeploy            | -                      |

| API                                                                                   | Action                               | Dependencies      |
|---------------------------------------------------------------------------------------|--------------------------------------|-------------------|
| GET /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}/prices | rf:stack:estimateExecution-PlanPrice | bss:discount:view |
| PATCH /v1/{project_id}/stacks/{stack_name}                                            | rf:stack:update                      | iam:agencies:pass |
| POST /v1/stack-sets                                                                   | rf:stackSet:create                   | iam:agencies:pass |
| GET /v1/stack-sets                                                                    | rf:stackSet:list                     | -                 |
| GET /v1/stack-sets/{stack_set_name}/templates                                         | rf:stackSet:showTemplate             | -                 |
| GET /v1/stack-sets/{stack_set_name}/metadata                                          | rf:stackSet:showMetadata             | -                 |
| POST /v1/stack-sets/{stack_set_name}/deployments                                      | rf:stackSet:deploy                   | -                 |
| DELETE /v1/stack-sets/{stack_set_name}                                                | rf:stackSet:delete                   | -                 |
| PATCH /v1/stack-sets/{stack_set_name}                                                 | rf:stackSet:update                   | iam:agencies:pass |
| GET /v1/stack-sets/{stack_set_name}/stack-instances                                   | rf:stackSet:listStackInstances       | -                 |
| GET /v1/stack-sets/{stack_set_name}/operations/{stack_set_operation_id}/metadata      | rf:stackSet:showOperationMetadata    | -                 |
| GET /v1/stack-sets/{stack_set_name}/operations                                        | rf:stackSet:listOperations           | -                 |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-280](#), the resource URN must be

specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for IAC.

**Table 3-280** Resource types supported by IAC

| Resource Type   | URN                                                               |
|-----------------|-------------------------------------------------------------------|
| privateTemplate | rf:<region>:<account-id>:privateTemplate:<template-name>          |
| stackSet        | rf:<region>:<account-id>:stackSet:<stack-set-name>/<stack-set-id> |
| stack           | rf:<region>:<account-id>:stack:<stack-name>                       |

## Conditions

IAC does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.14.13 Security Token Service (STS)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by STS, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by STS, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for STS.

**Table 3-281** Actions supported by STS

| Action                          | Description                                                                                                                                               | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                     | Alias |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| sts:agencies:assume             | Grants permission to obtain a set of temporary credentials that you can use to access resources that you might not normally have access to.               | Write        | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                                                                                                                                                                                                     | -     |
|                                 |                                                                                                                                                           |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">sts:ExternalId</a></li> <li>• <a href="#">sts:SourceIdentity</a></li> <li>• <a href="#">sts:TransitiveTagKeys</a></li> <li>• <a href="#">sts:AgencySessionName</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:SourceAccount</a></li> <li>• <a href="#">g:SourceUrn</a></li> </ul> |       |
| sts::decodeAuthorizationMessage | Grants permission to decode additional information about the authorization status of a request from an encoded message returned in response to a request. | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                 | -     |
| sts::setSourceIdentity          | Grants permission to set a source identity on a STS session.                                                                                              | Write        | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                                                                                                                                                                                                                                                     | -     |
|                                 |                                                                                                                                                           |              | -                           | <a href="#">sts:SourceIdentity</a>                                                                                                                                                                                                                                                                                                                                                                                |       |

| Action                        | Description                                        | Access Level | Resource Type (*: required) | Condition Key                                                                                                                                                                          | Alias |
|-------------------------------|----------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| sts::tagSession               | Grants permission to add tags to a STS session.    | Tagging      | agency *                    | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                                                                          | -     |
|                               |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">sts:TransitiveTagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li>• <a href="#">g:TagKeys</a></li> </ul> |       |
| sts::createServiceBearerToken | Grants permission to get the service bearer token. | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">sts:DurationTime</a></li> <li>• <a href="#">sts:ServiceName</a></li> </ul>                                                        | -     |

Each API of STS usually supports one or more actions. [Table 3-282](#) lists the supported actions and dependencies.

**Table 3-282** Actions and dependencies supported by STS APIs

| API                                   | Action                           | Dependencies                                                                                        |
|---------------------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------|
| POST /v5/agencies/assume              | sts:agencies:assume              | <ul style="list-style-type: none"> <li>• sts:tagSession</li> <li>• sts:setSourceIdentity</li> </ul> |
| POST /v5/decode-authorization-message | sts::decodeAuthorization-Message | -                                                                                                   |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-283](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for STS.

**Table 3-283** Resource types supported by STS

| Resource Type  | URN                                                           |
|----------------|---------------------------------------------------------------|
| agency         | iam::<account-id>:agency:<agency-name-with-path>              |
| assumed-agency | sts::<account-id>:assumed-agency:<agency-name>/<session-name> |

## Conditions

### Condition Key Overview

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the g: prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, sts) apply only to operations of the xx service. For details, see [Table 3-284](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [operators](#).

### Service-specific condition keys supported by STS

The following table lists the condition keys that you can define in identity policies for STS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-284** Service-specific condition keys supported by STS

| Service-specific Condition Key | Type    | Single-valued/<br>Multivalued | Description                                                                   |
|--------------------------------|---------|-------------------------------|-------------------------------------------------------------------------------|
| sts:ExternalId                 | string  | Single-valued                 | Filters access by the external ID that is passed in the request.              |
| sts:SourceIdentity             | string  | Single-valued                 | Filters access by the source identity that is passed in the request.          |
| sts:TransitiveTagKeys          | string  | Multivalued                   | Filters access by the transitive tag keys that are passed in the request.     |
| sts:AgencySessionName          | string  | Single-valued                 | Filters access by the agency session name required when you assume an agency. |
| sts:DurationTime               | numeric | Single-valued                 | Filters access by the duration times when you create a bearer token.          |
| sts:ServiceName                | string  | Single-valued                 | Filters access by the service name when you create a bearer token.            |

### 3.14.14 IAM Access Analyzer (IAA)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.



- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by IAM Access Analyzer, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by IAM Access Analyzer, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for IAM Access Analyzer.

**Table 3-285** Actions supported by IAM Access Analyzer

| Action                             | Description                                                          | Access Level | Resource Type (*: required) | Condition Key                                                                                     | Alias |
|------------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------|-------|
| AccessAnalyzer:analyzer:create     | Grants permission to create an access analyzer.                      | Write        | analyzer *                  | -                                                                                                 | -     |
|                                    |                                                                      |              | -                           | <ul style="list-style-type: none"> <li>g:RequestTag/&lt;tag-key&gt;</li> <li>g:TagKeys</li> </ul> |       |
| AccessAnalyzer:analyzer:get        | Grants permission to retrieve the access analyzer information.       | Read         | analyzer *                  | g:ResourceTag/<tag-key>                                                                           | -     |
| AccessAnalyzer:analyzer:list       | Grants permission to retrieve the access analyzer list.              | List         | analyzer *                  | -                                                                                                 | -     |
| AccessAnalyzer:analyzer:delete     | Grants permission to delete an access analyzer.                      | Write        | analyzer *                  | g:ResourceTag/<tag-key>                                                                           | -     |
| AccessAnalyzer:analyzer:update     | Grants permission to update the specified access analyzer.           | Write        | analyzer *                  | g:ResourceTag/<tag-key>                                                                           | -     |
| AccessAnalyzer:analyzer:scan       | Grants permission to start a scan for the specified access analyzer. | Write        | analyzer *                  | g:ResourceTag/<tag-key>                                                                           | -     |
| AccessAnalyzer:analyzer:getFinding | Grants permission to retrieve findings.                              | Read         | analyzer *                  | g:ResourceTag/<tag-key>                                                                           | -     |

| Action                                  | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                                                                                                     | Alias |
|-----------------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| AccessAnalyzer::analyzer:listFindings   | Grants permission to retrieve the finding list.                                   | List         | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| AccessAnalyzer::analyzer:updateFindings | Grants permission to update the findings.                                         | Write        | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
| AccessAnalyzer::tagResource             | Grants permission to add a tag to a resource.                                     | Tagging      | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                         |                                                                                   |              | -                           | <ul style="list-style-type: none"> <li><a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> <li><a href="#">g:TagKeys</a></li> </ul> |       |
| AccessAnalyzer::untagResource           | Grants permission to remove a tag from a resource.                                | Tagging      | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                     | -     |
|                                         |                                                                                   |              | -                           | <a href="#">g:TagKeys</a>                                                                                                         |       |
| AccessAnalyzer::archiveRule:create      | Grants permission to create an archive rule for the specified access analyzer.    | Write        | archiveRule *               | -                                                                                                                                 | -     |
| AccessAnalyzer::archiveRule:get         | Grants permission to retrieve the archive rule for the specified access analyzer. | Read         | archiveRule *               | -                                                                                                                                 | -     |

| Action                                | Description                                                                            | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|---------------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| AccessAnalyzer:archiveRule:list       | Grants permission to retrieve the archive rule list for the specified access analyzer. | List         | archiveRule *               | -                                             | -     |
| AccessAnalyzer:archiveRule:update     | Grants permission to modify the archive rule for the specified access analyzer.        | Write        | archiveRule *               | -                                             | -     |
| AccessAnalyzer:archiveRule:delete     | Grants permission to delete the archive rule for the specified access analyzer.        | Write        | archiveRule *               | -                                             | -     |
| AccessAnalyzer:archiveRule:apply      | Grants permission to apply an archive rule.                                            | Write        | archiveRule *               | -                                             | -     |
| AccessAnalyzer:analyzer:createPreview | Grants permission to create an access preview for the specified access analyzer.       | Write        | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                                               | Description                                                                                     | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| AccessAnalyzer:analyzer:get Preview                  | Grants permission to retrieve the access preview information for the specified access analyzer. | Read         | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| AccessAnalyzer:analyzer:list Previews                | Grants permission to retrieve the access preview list for the specified access analyzer.        | List         | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| AccessAnalyzer:analyzer:list PreviewFindings         | Grants permission to retrieve the preview finding list for the specified access analyzer.       | List         | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| AccessAnalyzer:analyzer:createResourceConfigurations | Grants permission to create or update resource configurations.                                  | Write        | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| AccessAnalyzer:analyzer:list ResourceConfigurations  | Grants permission to retrieve the list for resource configurations.                             | List         | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |

| Action                                                | Description                                                                       | Access Level | Resource Type (*: required) | Condition Key                                 | Alias |
|-------------------------------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------|
| AccessAnalyzer::analyzer:deleteResourceConfigurations | Grants permission to delete the resource configurations.                          | Write        | analyzer *                  | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> | -     |
| AccessAnalyzer::validatePolicy                        | Grants permission to validate a policy.                                           | Read         | -                           | -                                             | -     |
| AccessAnalyzer::checkNoNewAccess                      | Grants permission to check whether the updated policy has new access permissions. | Read         | -                           | -                                             | -     |
| AccessAnalyzer::notificationSetting:list              | Grants permission to retrieve the notification setting list.                      | Read         | notificationSetting *       | -                                             | -     |
| AccessAnalyzer::notificationSetting:create            | Grants permission to create a notification setting.                               | Write        | notificationSetting *       | -                                             | -     |
| AccessAnalyzer::notificationSetting:get               | Grants permission to retrieve the notification setting.                           | Read         | notificationSetting *       | -                                             | -     |
| AccessAnalyzer::notificationSetting:update            | Grants permission to modify the notification setting.                             | Write        | notificationSetting *       | -                                             | -     |

| Action                                    | Description                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| AccessAnalyzer:notificationSetting:delete | Grants permission to delete the notification setting. | Write        | notificationSetting *       | -             | -     |

Each API of IAM Access Analyzer usually supports one or more actions. [Table 3-286](#) lists the supported actions and dependencies.

**Table 3-286** Actions and dependencies supported by IAM Access Analyzer APIs

| API                                                   | Action                                 | Dependencies                             |
|-------------------------------------------------------|----------------------------------------|------------------------------------------|
| POST /v5/analyzers                                    | AccessAnalyzer:analyzer:create         | iam:agencies:createServiceLinkedAgencyV5 |
| GET /v5/analyzers/{analyzer_id}                       | AccessAnalyzer:analyzer:get            | -                                        |
| GET /v5/analyzers                                     | AccessAnalyzer:analyzer:list           | -                                        |
| DELETE /v5/analyzers/{analyzer_id}                    | AccessAnalyzer:analyzer:delete         | -                                        |
| PUT /v5/analyzers/{analyzer_id}                       | AccessAnalyzer:analyzer:update         | -                                        |
| POST /v5/analyzers/{analyzer_id}/scan                 | AccessAnalyzer:analyzer:scan           | -                                        |
| GET /v5/analyzers/{analyzer_id}/findings/{finding_id} | AccessAnalyzer:analyzer:getFinding     | -                                        |
| POST /v5/analyzers/{analyzer_id}/findings             | AccessAnalyzer:analyzer:listFindings   | -                                        |
| PUT /v5/analyzers/{analyzer_id}/findings              | AccessAnalyzer:analyzer:updateFindings | -                                        |

| API                                                                    | Action                                | Dependencies |
|------------------------------------------------------------------------|---------------------------------------|--------------|
| POST /v5/{resource_type}/{resource_id}/tags/create                     | AccessAnalyzer::tagResource           | -            |
| POST /v5/{resource_type}/{resource_id}/tags/delete                     | AccessAnalyzer::untagResource         | -            |
| POST /v5/analyzers/{analyzer_id}/archive-rules                         | AccessAnalyzer:archiveRule:create     | -            |
| GET /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}        | AccessAnalyzer:archiveRule:get        | -            |
| GET /v5/analyzers/{analyzer_id}/archive-rules                          | AccessAnalyzer:archiveRule:list       | -            |
| PUT /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}        | AccessAnalyzer:archiveRule:update     | -            |
| DELETE /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}     | AccessAnalyzer:archiveRule:delete     | -            |
| POST /v5/analyzers/{analyzer_id}/archive-rules/{archive_rule_id}/apply | AccessAnalyzer:archiveRule:apply      | -            |
| POST /v5/analyzers/{analyzer_id}/access-previews                       | AccessAnalyzer:analyzer:createPreview | -            |
| GET /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}    | AccessAnalyzer:analyzer:getPreview    | -            |
| GET /v5/analyzers/{analyzer_id}/access-previews                        | AccessAnalyzer:analyzer:listPreviews  | -            |



| API                                                                           | Action                                                 | Dependencies |
|-------------------------------------------------------------------------------|--------------------------------------------------------|--------------|
| POST /v5/analyzers/{analyzer_id}/access-previews/{access_preview_id}/findings | AccessAnalyzer:analyzer:list<br>PreviewFindings        | -            |
| POST /v5/analyzers/{analyzer_id}/resource-configurations/create               | AccessAnalyzer:analyzer:createResourceConfigurations   | -            |
| GET /v5/analyzers/{analyzer_id}/resource-configurations                       | AccessAnalyzer:analyzer:list<br>ResourceConfigurations | -            |
| POST /v5/analyzers/{analyzer_id}/resource-configurations/delete               | AccessAnalyzer:analyzer:deleteResourceConfigurations   | -            |
| POST /v5/policies/validate                                                    | AccessAnalyzer::validatePolicy                         | -            |
| POST /v5/policies/check-no-new-access                                         | AccessAnalyzer::checkNoNewAccess                       | -            |
| GET /v5/notification-settings                                                 | AccessAnalyzer:notification<br>Setting:list            | -            |
| POST /v5/notification-settings                                                | AccessAnalyzer:notification<br>Setting:create          | -            |
| GET /v5/notification-settings/{notification_setting_id}                       | AccessAnalyzer:notification<br>Setting:get             | -            |
| PUT /v5/notification-settings/{notification_setting_id}                       | AccessAnalyzer:notification<br>Setting:update          | -            |
| DELETE /v5/notification-settings/{notification_setting_id}                    | AccessAnalyzer:notification<br>Setting:delete          | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-287](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for IAM Access Analyzer.

**Table 3-287** Resource types supported by IAM Access Analyzer

| Resource Type       | URN                                                                                |
|---------------------|------------------------------------------------------------------------------------|
| analyzer            | AccessAnalyzer:<region>:<account-id>:analyzer:<analyzer-id>                        |
| notificationSetting | AccessAnalyzer:<region>:<account-id>:notificationSetting:<notification-setting-id> |
| archiveRule         | AccessAnalyzer:<region>:<account-id>:archiveRule:<analyzer-id>/<archive-rule-id>   |

## Conditions

IAM Access Analyzer does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.14.15 Resource Governance Center (RGC)

IAM provides system-defined identity policies to define typical cloud service permissions. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by RGC, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by RGC, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for RGC.

**Table 3-288** Actions supported by RGC

| Action                    | Description                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:control:list          | Grants permission to list governance policies.                            | List         | -                           | -             | -     |
| rgc:controlViolation:list | Grants permission to list non-compliant resources.                        | List         | -                           | -             | -     |
| rgc:control:get           | Grants permission to get the details about a governance policy.           | Read         | -                           | -             | -     |
| rgc:control:enable        | Grants permission to enable a governance policy.                          | Write        | -                           | -             | -     |
| rgc:control:disable       | Grants permission to disable a governance policy.                         | Write        | -                           | -             | -     |
| rgc:controlOperate:get    | Grants permission to identify the enabling status of a governance policy. | Read         | -                           | -             | -     |

| Action                                 | Description                                                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:enabledControl:list                | Grants permission to list governance policies enabled for an organization.                                | List         | -                           | -             | -     |
| rgc:controlsForOrganizationalUnit:list | Grants permission to list governance policies enabled for an organizational unit.                         | List         | -                           | -             | -     |
| rgc:controlsForAccount:list            | Grants permission to list governance policies enabled for an account.                                     | List         | -                           | -             | -     |
| rgc:complianceStatusForAccount:get     | Grants permission to identify the compliance status of resources in a managed account in an organization. | Read         | -                           | -             | -     |

| Action                                        | Description                                                                                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:complianceStatusForOrganizationalUnit:get | Grants permission to identify the compliance status of resources in all managed accounts in a registered organizational unit in an organization. | Read         | -                           | -             | -     |
| rgc:controlsForOrganizationalUnit:get         | Grants permission to get the details about governance policies enabled for a registered organizational unit in an organization.                  | Read         | -                           | -             | -     |
| rgc:controlsForAccount:get                    | Grants permission to get the details about governance policies enabled for a managed account in an organization.                                 | Read         | -                           | -             | -     |
| rgc:configRuleCompliance:list                 | Grants permission to list managed accounts for compliance against Config rules.                                                                  | List         | -                           | -             | -     |

| Action                                   | Description                                                                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:externalConfigRuleCompliance:list    | Grants permission to list managed accounts for compliance against external Config rules.                               | List         | -                           | -             | -     |
| rgc:driftDetail:list                     | Grants permission to list the drift summary of the landing zone.                                                       | List         | -                           | -             | -     |
| rgc:managedOrganizationalUnit:register   | Grants permission to register an organizational unit.                                                                  | Write        | -                           | -             | -     |
| rgc:managedOrganizationalUnit:reRegister | Grants permission to re-register an organizational unit.                                                               | Write        | -                           | -             | -     |
| rgc:managedOrganizationalUnit:deregister | Grants permission to deregister an organizational unit.                                                                | Write        | -                           | -             | -     |
| rgc:operation:get                        | Grants permission to get the details about registration, re-registration, or deregistration of an organizational unit. | Read         | -                           | -             | -     |

| Action                               | Description                                                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:managedOrganizationalUnit:delete | Grants permission to delete an organizational unit.                                                       | Write        | -                           | -             | -     |
| rgc:managedOrganizationalUnit:get    | Grants permission to get the details about a registered organizational unit.                              | Read         | -                           | -             | -     |
| rgc:managedOrganizationalUnit:create | Grants permission to create an organizational unit.                                                       | Write        | -                           | -             | -     |
| rgc:managedOrganizationalUnit:list   | Grants permission to list registered organizational units that governance policies have been enabled for. | List         | -                           | -             | -     |
| rgc:managedAccount:enroll            | Grants permission to manage an account.                                                                   | Write        | -                           | -             | -     |
| rgc:managedAccount:unenroll          | Grants permission to unmanage an account.                                                                 | Write        | -                           | -             | -     |
| rgc:managedAccount:update            | Grants permission to update a managed account.                                                            | Write        | -                           | -             | -     |



| Action                            | Description                                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:managedAccount:get            | Grants permission to get the details about a managed account.                              | Read         | -                           | -             | -     |
| rgc:managedAccountsForParent:list | Grants permission to list managed accounts in a registered organizational unit.            | List         | -                           | -             | -     |
| rgc:managedAccount:create         | Grants permission to create an account.                                                    | Write        | -                           | -             | -     |
| rgc:managedAccount:list           | Grants permission to list managed accounts that governance policies have been enabled for. | List         | -                           | -             | -     |
| rgc:managedCoreAccount:get        | Grants permission to get the details about a managed core account.                         | Read         | -                           | -             | -     |
| rgc:homeRegion:get                | Grants permission to get the details about the home region of the landing zone.            | Read         | -                           | -             | -     |

| Action                           | Description                                                                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------|--------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:preLaunch:check              | Grants permission to check whether the current region is eligible for setting up a landing zone. | Write        | -                           | -             | -     |
| rgc:landingZone:setup            | Grants permission to set up a landing zone.                                                      | Write        | -                           | -             | -     |
| rgc:landingZone:delete           | Grants permission to delete a landing zone.                                                      | Write        | -                           | -             | -     |
| rgc:landingZoneStatus:get        | Grants permission to identify the status of landing zone setup.                                  | Read         | -                           | -             | -     |
| rgc:availableUpdate:get          | Grants permission to identify the available updates of a landing zone.                           | Read         | -                           | -             | -     |
| rgc:landingZoneConfiguration:get | Grants permission to get the configurations of a landing zone.                                   | Read         | -                           | -             | -     |

| Action                             | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:landingZonelidentityCenter:get | Grants permission to get the details about IAM Identity Center users of a landing zone.           | Read         | -                           | -             | -     |
| rgc:operation:list                 | Grants permission to obtain the current operation status of a registered OU or a managed account. | List         | -                           | -             | -     |
| rgc:templateDeployParam:get        | Grants permission to show the deploy parameters of the template.                                  | Read         | -                           | -             | -     |
| rgc:template:create                | Grants permission to create template.                                                             | Write        | -                           | -             | -     |
| rgc:template:delete                | Grants permission to delete template.                                                             | Write        | -                           | -             | -     |
| rgc:predefinedTemplate:list        | Grants permission to list the predefined templates.                                               | List         | -                           | -             | -     |

| Action                         | Description                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| rgc:managedAccountTemplate:get | Grants permission to get the template details about a managed account. | Read         | -                           | -             | -     |

Each API of RGC usually supports one or more actions. [Table 3-289](#) lists the supported actions and dependencies.

**Table 3-289** Actions and dependencies supported by RGC APIs

| API                                                                       | Action                    | Dependencies |
|---------------------------------------------------------------------------|---------------------------|--------------|
| GET /v1/governance/controls                                               | rgc:control:list          | -            |
| GET /v1/governance/control-violations                                     | rgc:controlViolation:list | -            |
| GET /v1/governance/controls/{control_id}                                  | rgc:control:get           | -            |
| POST /v1/governance/controls/enable                                       | rgc:control:enable        | -            |
| POST /v1/governance/controls/disable                                      | rgc:control:disable       | -            |
| GET /v1/governance/operation-control-status/{operation_control_status_id} | rgc:controlOperate:get    | -            |
| GET /v1/governance/enabled-controls                                       | rgc:enabledControl:list   | -            |

| API                                                                                                    | Action                                        | Dependencies |
|--------------------------------------------------------------------------------------------------------|-----------------------------------------------|--------------|
| GET /v1/governance/managed-organizational-units/{managed_organizational_unit_id}/controls              | rgc:controlsForOrganizationalUnit:list        | -            |
| GET /v1/governance/managed-accounts/{managed_account_id}/controls                                      | rgc:controlsForAccount:list                   | -            |
| GET /v1/governance/managed-accounts/{managed_account_id}/compliance-status                             | rgc:complianceStatusForAccount:get            | -            |
| GET /v1/governance/managed-organizational-units/{managed_organizational_unit_id}/compliance-status     | rgc:complianceStatusForOrganizationalUnit:get | -            |
| GET /v1/governance/managed-organizational-units/{managed_organizational_unit_id}/controls/{control_id} | rgc:controlsForOrganizationalUnit:get         | -            |
| GET /v1/governance/managed-accounts/{managed_account_id}/controls/{control_id}                         | rgc:controlsForAccount:get                    | -            |

| API                                                                                                     | Action                                   | Dependencies |
|---------------------------------------------------------------------------------------------------------|------------------------------------------|--------------|
| GET /v1/governance/managed-accounts/{managed_account_id}/config-rule-compliances                        | rgc:configRuleCompliance:list            | -            |
| GET /v1/governance/managed-accounts/{managed_account_id}/external-config-rule-compliances               | rgc:externalConfigRuleCompliance:list    | -            |
| GET /v1/governance/drift-details                                                                        | rgc:driftDetail:list                     | -            |
| POST /v1/managed-organization/organizational-units/{organizational_unit_id}/register                    | rgc:managedOrganizationalUnit:register   | -            |
| POST /v1/managed-organization/organizational-units/{organizational_unit_id}/re-register                 | rgc:managedOrganizationalUnit:reRegister | -            |
| POST /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}/de-register | rgc:managedOrganizationalUnit:deRegister | -            |
| GET /v1/managed-organization/{operation_id}                                                             | rgc:operation:get                        | -            |
| DELETE /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}           | rgc:managedOrganizationalUnit:delete     | -            |

| API                                                                                                         | Action                               | Dependencies |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------|--------------|
| GET /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}                  | rgc:managedOrganizationalUnit:get    | -            |
| POST /v1/managed-organization/managed-organizational-units                                                  | rgc:managedOrganizationalUnit:create | -            |
| GET /v1/managed-organization/managed-organizational-units                                                   | rgc:managedOrganizationalUnit:list   | -            |
| POST /v1/managed-organization/accounts/{managed_account_id}/enroll                                          | rgc:managedAccount:enroll            | -            |
| POST /v1/managed-organization/managed-accounts/{managed_account_id}/un-enroll                               | rgc:managedAccount:unEnroll          | -            |
| POST /v1/managed-organization/managed-accounts/{managed_account_id}/update                                  | rgc:managedAccount:update            | -            |
| GET /v1/managed-organization/managed-accounts/{managed_account_id}                                          | rgc:managedAccount:get               | -            |
| GET /v1/managed-organization/managed-organizational-units/{managed_organizational_unit_id}/managed-accounts | rgc:managedAccountsForParent:list    | -            |

| API                                                 | Action                            | Dependencies |
|-----------------------------------------------------|-----------------------------------|--------------|
| POST /v1/managed-organization/managed-accounts      | rgc:managedAccount:create         | -            |
| GET /v1/managed-organization/managed-accounts       | rgc:managedAccount:list           | -            |
| GET /v1/managed-organization/managed-core-accounts  | rgc:managedCoreAccount:get        | -            |
| GET /v1/landing-zone/home-region                    | rgc:homeRegion:get                | -            |
| POST /v1/landing-zone/pre-launch-check              | rgc:preLaunch:check               | -            |
| POST /v1/landing-zone/setup                         | rgc:landingZone:setup             | -            |
| POST /v1/landing-zone/delete                        | rgc:landingZone:delete            | -            |
| GET /v1/landing-zone/status                         | rgc:landingZoneStatus:get         | -            |
| GET /v1/landing-zone/available-updates              | rgc:availableUpdate:get           | -            |
| GET /v1/landing-zone/configuration                  | rgc:landingZoneConfiguration:get  | -            |
| GET /v1/landing-zone/identity-center                | rgc:landingZoneIdentityCenter:get | -            |
| GET /v1/managed-organization                        | rgc:operation:list                | -            |
| GET /v1/rgc/templates/{template_name}/deploy-params | rgc:templateDeployParam:get       | -            |
| POST /v1/rgc/templates                              | rgc:template:create               | -            |
| DELETE /v1/rgc/templates/{template_name}            | rgc:template:delete               | -            |



| API                                                                          | Action                         | Dependencies |
|------------------------------------------------------------------------------|--------------------------------|--------------|
| GET /v1/rgc/predefined-templates                                             | rgc:predefinedTemplate:list    | -            |
| GET /v1/managed-organization/managed-accounts/{managed_account_id}/blueprint | rgc:managedAccountTemplate:get | -            |

## Resources

RGC does not support resource-level authorization. To allow access to RGC, use a wildcard (\*) in the Resource element of the identity policy, indicating that the identity policy will be applied to all resources.

## Conditions

RGC does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.14.16 Cloud Operations Center (COC)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, [Service Control Policies \(SCPs\)](#) in [Organizations](#) can also use these actions to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the entity. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted IAM permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by COC, see [Resource Types \(Resource\)](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by COC, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for COC.

**Table 3-290** Actions supported by COC

| Action               | Description                                            | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------|--------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:application:list | Provides the permission to query the application list. | List         | application *               | -             | -     |

| Action                            | Description                                                          | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:application:create            | Provides the permission to create an application.                    | Write        | application *               | -             | -     |
| coc:application:update            | Provides the permission to modify an application.                    | Write        | application *               | -             | -     |
| coc:application:delete            | Provides the permission to delete an application.                    | Write        | application *               | -             | -     |
| coc:application:createGroup       | Provides the permission to create an application group.              | Write        | application *               | -             | -     |
| coc:application:listGroups        | Provides the permission to query a specified application group list. | List         | application *               | -             | -     |
| coc:application:updateGroup       | Provides the permission to modify an application group.              | Write        | application *               | -             | -     |
| coc:application:deleteGroup       | Provides the permission to delete an application group.              | Write        | application *               | -             | -     |
| coc:application:syncGroupResource | Provides the permissions to synchronize application group resources. | Write        | application *               | -             | -     |
| coc:application:updateResources   | Provides the permission to modify application resources.             | Write        | application *               | -             | -     |

| Action                                 | Description                                                                             | Access Level | Resource Type (*: Required) | Condition Key                            | Alias |
|----------------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------------|-------|
| coc:application:addResources           | Provides the permission to add resources to an application.                             | Write        | application *               | -                                        | -     |
| coc:application:removeResources        | Provides the permission to remove application resources.                                | Write        | application *               | -                                        | -     |
| coc:application:listResources          | Provides the permission to query the application resource list.                         | List         | application *               | -                                        | -     |
|                                        |                                                                                         |              | -                           | <a href="#">coc:ApplicationGroupCode</a> |       |
| coc:application:countResourceRelations | Provides the permission to query the number of resource relationships.                  | List         | application *               | -                                        | -     |
| coc:application:getCapacity            | Provides the permission to query resource capacities in an application.                 | List         | application *               | -                                        | -     |
| coc:application:getSortedCapacity      | Provides the permission to query the capacities of ordered resources in an application. | List         | application *               | -                                        | -     |
| coc:application:listModel              | Provides the permission to query application models.                                    | List         | application *               | -                                        | -     |
| coc:vendorAccount:create               | Provides the permission to add a cloud vendor account.                                  | Write        | -                           | -                                        | -     |

| Action                         | Description                                                                           | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:vendorAccount:list         | Provides the permission to query a cloud vendor account.                              | List         | -                           | -             | -     |
| coc:vendorAccount:update       | Provides the permission to modify a cloud vendor account.                             | Write        | -                           | -             | -     |
| coc:vendorAccount:delete       | Provides the permission to delete a cloud vendor account.                             | Write        | -                           | -             | -     |
| coc:resourceView:list          | Provides the permission to query resource views.                                      | List         | -                           | -             | -     |
| coc:resourceView:create        | Provides the permission to create a resource view.                                    | Write        | resource View *             | -             | -     |
| coc:resourceView:update        | Provides the permission to update a resource view.                                    | Write        | resource View *             | -             | -     |
| coc:resourceView:delete        | Provides the permission to delete a resource view.                                    | Write        | resource View *             | -             | -     |
| coc:resourceView:syncResources | Provides the permission to synchronize the resource list in a specific resource view. | Write        | resource View *             | -             | -     |

| Action                           | Description                                                                                                       | Access Level | Resource Type (*: Required) | Condition Key | Alias                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------|
| coc:resourceView:listResources   | Provides the permission to query the resource list in a specific resource view.                                   | List         | resourceView*               | -             | -                               |
| coc:resourceView:countResources  | Provides the permission to query the number of resources in a specific resource view.                             | List         | -                           | -             | -                               |
| coc:instance:listResources       | Provides the permission to query the resource list.                                                               | List         | -                           | -             | -                               |
| coc:instance:syncResources       | Provides the permission to synchronize the resource list.                                                         | Write        | -                           | -             | -                               |
| coc:instance:countOtherResources | Provides the permission to query the total number of offline resources (such as physical machine and middleware). | List         | -                           | -             | -                               |
| coc:instance:listTagsForResource | Provides the permission to query resource tags.                                                                   | List         | -                           | -             | coc:instance:listResourceTags   |
| coc:instance:addResourceToTags   | Provides the permission to add resource tags.                                                                     | Write        | -                           | -             | coc:instance:createResourceTags |
| coc:instance:countResources      | Provides the permission to query the total number of resources.                                                   | List         | -                           | -             | -                               |

| Action                        | Description                                                                        | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                               | Alias                               |
|-------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| coc::listEpsCollection        | Provides the permission to query the favorited enterprise projects.                | List         | -                           | -                                                                                                                                                           | coc:enterpriseProject:listCollect   |
| coc::updateEpsCollection      | Provides the permission to modify the favorited enterprise projects.               | Write        | -                           | -                                                                                                                                                           | coc:enterpriseProject:updateCollect |
| coc::getLastSyncStatus        | Provides the permission to query the latest synchronization status of an instance. | Read         | -                           | -                                                                                                                                                           | coc:system:getLastSyncStatus        |
| coc::getResourceSyncJobDetail | Provides the permission to query details about a resource synchronization task.    | Read         | -                           | -                                                                                                                                                           | coc:system:getResourceSyncJobDetail |
| coc:schedule:create           | Provides the permission to create a scheduled task.                                | Write        | schedule                    | <b>g:EnterpriseProjectId</b>                                                                                                                                | -                                   |
|                               |                                                                                    |              | instance                    | <ul style="list-style-type: none"> <li><b>coc:ApplicationCode</b></li> <li><b>coc:ApplicationGroupCode</b></li> <li><b>g:EnterpriseProjectId</b></li> </ul> |                                     |
|                               |                                                                                    |              | document                    | <ul style="list-style-type: none"> <li><b>coc:DocumentRiskLevel</b></li> <li><b>g:EnterpriseProjectId</b></li> </ul>                                        |                                     |

| Action              | Description                                        | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|---------------------|----------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                     |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:schedule:list   | Provides the permission to query scheduled tasks.  | List         | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -     |
| coc:schedule:update | Provides the permission to update scheduled tasks. | Write        | schedule*                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -     |



| Action              | Description                                              | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                | Alias |
|---------------------|----------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                     |                                                          |              | instance                    | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:ApplicationGroupCode</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> |       |
|                     |                                                          |              | document                    | <ul style="list-style-type: none"> <li>• <a href="#">coc:DocumentRiskLevel</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                   |       |
| coc:schedule:get    | Provides the permission to query scheduled task details. | Read         | schedule*                   | -                                                                                                                                                                                            | -     |
|                     |                                                          |              | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                        |       |
| coc:schedule:delete | Provides the permission to delete a scheduled task.      | Write        | schedule*                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                        | -     |
| coc:schedule:enable | Provides the permission to enable a scheduled task.      | Write        | schedule*                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                        | -     |

| Action                    | Description                                                                 | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|---------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                           |                                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:schedule:disable      | Provides the permission to disable a scheduled task.                        | Write        | schedule*                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -     |
| coc:schedule:getHistories | Provides the permission to query the execution history of a scheduled task. | Read         | schedule*                   | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -     |

| Action                              | Description                                                                  | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                | Alias |
|-------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:instance:executeDocument        | Provides the permission to execute documents on an ECS.                      | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:ApplicationGroupCode</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -     |
|                                     |                                                                              |              | document *                  | <ul style="list-style-type: none"> <li>• <a href="#">g:EnterpriseProjectId</a></li> <li>• <a href="#">coc:DocumentRiskLevel</a></li> </ul>                                                   |       |
| coc:alarm:clear                     | Provides the permission to clear alarms.                                     | Write        | -                           | -                                                                                                                                                                                            | -     |
| coc:alarm:createAlarmLinkedIncident | Provides the permission to create incidents that are associated with alarms. | Write        | -                           | -                                                                                                                                                                                            | -     |
| coc:alarm:listHandleHistories       | Provides the permission to query the alarm handling history.                 | List         | -                           | -                                                                                                                                                                                            | -     |
| coc:alarm:get                       | Provides the permission to query alarm information.                          | Read         | -                           | -                                                                                                                                                                                            | -     |
| coc:ticket:list                     | Provides the permission to query incident tickets.                           | List         | -                           | -                                                                                                                                                                                            | -     |
| coc:ticket:create                   | Provides the permission to create incident tickets.                          | Write        | -                           | -                                                                                                                                                                                            | -     |

| Action                           | Description                                                                 | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------|-----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:ticket:get                   | Provides the permission to query incident ticket details.                   | Read         | -                           | -             | -     |
| coc:ticket:action                | Provides the permission to process incident tickets.                        | Write        | -                           | -             | -     |
| coc:ticket:delete                | Provides the permission to delete incident tickets.                         | Write        | -                           | -             | -     |
| coc:ticket:upload File           | Provides the permission to upload attachments for incident tickets.         | Write        | -                           | -             | -     |
| coc:ticket:downloadFile          | Provides the permission to download attachments for incident tickets.       | Read         | -                           | -             | -     |
| coc:ticket:listAuthorizable      | Provides the permission to query authorized tickets.                        | List         | -                           | -             | -     |
| coc:warroom:create               | Provides the permission to create a war room.                               | Write        | -                           | -             | -     |
| coc:ticket:update                | Provides the permission to modify incident tickets.                         | Write        | -                           | -             | -     |
| coc:ticket:getOperationHistories | Provides the permission to query the operation history of incident tickets. | List         | -                           | -             | -     |

| Action                      | Description                                                                    | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:ticket:listActions      | Provides the permission to query the list of operations that can be performed. | List         | -                           | -             | -     |
| coc:warroom:list            | Provides the permission to query the war room list.                            | List         | -                           | -             | -     |
| coc:document:analyzeRisk    | Provides the permission to analyze document risks.                             | Read         | -                           | -             | -     |
| coc:document:get            | Provides the permission to view document content.                              | Read         | -                           | -             | -     |
| coc:document:getDocument    | Provides the permission to query document details.                             | Read         | document *                  | -             | -     |
| coc:document:create         | Provides the permission to create a document.                                  | Write        | document *                  | -             | -     |
| coc:document:createDocument | Provides the permission to create a document.                                  | Write        | document *                  | -             | -     |
| coc:document:delete         | Provides the permission to delete a document.                                  | Write        | document *                  | -             | -     |
| coc:document:deleteDocument | Provides the permission to delete a document.                                  | Write        | document *                  | -             | -     |

| Action                      | Description                                                       | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:document:execute        | Provides the permission to execute a document.                    | Write        | document *                  | -             | -     |
| coc:document:update         | Provides the permission to modify a document.                     | Write        | document *                  | -             | -     |
| coc:document:updateDocument | Provides the permission to update a document.                     | Write        | document *                  | -             | -     |
| coc:document:list           | Provides the permission to query the document list.               | List         | document *                  | -             | -     |
| coc:document:listDocument   | Provides the permission to query the document list.               | List         | -                           | -             | -     |
| coc:quota:get               | Provides the permission to query quotas.                          | Read         | -                           | -             | -     |
| coc:job:get                 | Provides the permission to query service ticket details.          | Read         | job *                       | -             | -     |
|                             |                                                                   |              | -                           | coc:JobType   |       |
| coc:job:action              | Provides the permission to perform operations on service tickets. | Write        | job *                       | -             | -     |
|                             |                                                                   |              | -                           | coc:JobType   |       |
| coc:job:list                | Provides the permission to query the service ticket list.         | List         | job *                       | -             | -     |
|                             |                                                                   | -            | -                           | coc:JobType   |       |

| Action                                   | Description                                                                     | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:instance:autoBatchInstances          | Provides the permission to automatically perform batch operations on instances. | Write        | -                           | -             | -     |
| coc:documentAtomic:list                  | Provides the permission to query the atomic capability list of a document.      | List         | -                           | -             | -     |
| coc:documentAtomic:get                   | Provides the permission to query details about a document atomic capability.    | Read         | -                           | -             | -     |
| coc:execution:get                        | Provides the permission to execute service ticket details.                      | Read         | -                           | -             | -     |
| coc:execution:listExecutionStep          | Provides the permission to query the list of service ticket execution steps.    | Read         | -                           | -             | -     |
| coc:execution:list                       | Provides the permission to query the service ticket list.                       | List         | -                           | -             | -     |
| coc:execution:listExecutionStepIn-stance | Provides the permission to query the list of service ticket execution steps.    | Read         | -                           | -             | -     |
| coc:execution:operate                    | Provides the permission to perform operations on a service ticket.              | Write        | -                           | -             | -     |

| Action                    | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:complianceReport:list | Provides the permission to query the compliance report list.        | List         | -                           | -             | -     |
| coc:complianceReport:get  | Provides the permission to query compliance report details.         | Read         | -                           | -             | -     |
| coc:task:list             | Provides the permission to query the O&M transaction list.          | List         | -                           | -             | -     |
| coc:task:count            | Provides the permission to query the number of O&M transactions.    | Read         | -                           | -             | -     |
| coc:task:create           | Provides the permission to create an O&M transaction.               | Write        | -                           | -             | -     |
| coc:task:get              | Provides the permission to query the details of an O&M transaction. | Read         | -                           | -             | -     |
| coc:task:accept           | Provides the permission to accept an O&M transaction.               | Write        | -                           | -             | -     |
| coc:task:complete         | Provides the permission to end an O&M transaction.                  | Write        | -                           | -             | -     |
| coc:task:cancel           | Provides the permission to cancel an O&M transaction.               | Write        | -                           | -             | -     |



| Action                   | Description                                      | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                            | Alias |
|--------------------------|--------------------------------------------------|--------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:tag:create           | Provides the permission to create a tag.         | Tagging      | -                           | -                                                                                                                                                                                        | -     |
| coc:tag:list             | Provides the permission to query tags.           | List         | -                           | -                                                                                                                                                                                        | -     |
| coc:instance:reinstallOS | Provides the permission to reinstall the ECS OS. | Write        | instance                    | <ul style="list-style-type: none"><li>• <a href="#">coc:ApplicationCode</a></li><li>• <a href="#">coc:ApplicationGroupCode</a></li><li>• <a href="#">g:EnterpriseProjectId</a></li></ul> | -     |

| Action                | Description                                         | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|-----------------------|-----------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                       |                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:instance:changeOS | Provides the permission to change the OS of an ECS. | Write        | instance                    | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:ApplicationGroupCode</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                | -     |

| Action                        | Description                                        | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|-------------------------------|----------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                               |                                                    |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:instance:scanOSCompliance | Provides the permission to scan server OS patches. | Read         | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:ApplicationGroupCode</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                | -     |

| Action                      | Description                                           | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias                     |
|-----------------------------|-------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| coc:instance:installPatches | Provides the permission to install patches on an ECS. | Write        | instance *                  | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> | -                         |
| coc::listSSHKeypairs        | Provides the permission to query SSH key pairs.       | List         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | coc:system:listSSHKeypair |
| coc:personnel:list          | Provides the permission to query personnel.           | List         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -                         |
| coc:personnel:add           | Provides the permission to add personnel.             | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -                         |

| Action                                 | Description                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------------|------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:personnel:update                   | Provides the permission to update personnel information.   | Write        | -                           | -             | -     |
| coc:personnel:remove                   | Provides the permission to remove personnel.               | Write        | -                           | -             | -     |
| coc:patchBaseline:create               | Provides the permission to create a patch baseline.        | Write        | -                           | -             | -     |
| coc:patchBaseline:list                 | Provides the permission to query the patch baseline list.  | List         | -                           | -             | -     |
| coc:patchBaseline:get                  | Provides the permission to query patch baseline details.   | Read         | -                           | -             | -     |
| coc:patchBaseline:opsSystemGet         | Provides the permission to obtain OS baselines.            | Read         | -                           | -             | -     |
| coc:patchBaseline:updateCustomBaseline | Provides the permission to update a custom baseline patch. | Write        | -                           | -             | -     |
| coc:patchBaseline:delete               | Provides the permission to delete a patch baseline.        | Write        | -                           | -             | -     |
| coc:patchBaseline:update               | Provides the permission to update a patch baseline.        | Write        | -                           | -             | -     |

| Action                               | Description                                                                    | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------------|--------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:patchBaseline:registerDefault    | Provides the permission to set the default patch baseline.                     | Write        | -                           | -             | -     |
| coc:patchBaseline:getDefault         | Provides the permission to query the default patch baseline.                   | Read         | -                           | -             | -     |
| coc:document:listRunbookAtomic       | Provides the permission to query the atomic capability list of custom jobs.    | List         | -                           | -             | -     |
| coc:document:getRunbookAtomicDetails | Provides the permission to query the atomic capability details of custom jobs. | Read         | -                           | -             | -     |
| coc:biStatistic:list                 | Provides the permission to query BI metric results.                            | Read         | -                           | -             | -     |
| coc:integration:list                 | Provides the permission to query the integration configuration list.           | List         | -                           | -             | -     |
| coc:integration:get                  | Provides the permission to query integration configuration details.            | Read         | -                           | -             | -     |
| coc:integration:update               | Provides the permission to modify integration configurations.                  | Write        | -                           | -             | -     |

| Action                     | Description                                                                                  | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------|----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:integration:access     | Provides the permission to access integration configurations.                                | Write        | -                           | -             | -     |
| coc:integration:enable     | Provides the permission to enable integration configurations.                                | Write        | -                           | -             | -     |
| coc:integration:disable    | Provides the permission to disable integration configurations.                               | Write        | -                           | -             | -     |
| coc:integration:remove     | Provides the permission to remove integration configurations.                                | Write        | -                           | -             | -     |
| coc:integration:getHistory | Provides the permission to query historical incident messages of integration configurations. | Read         | -                           | -             | -     |
| coc:ticket:getEnumTypes    | Provides the permission to query incident ticket enumeration type details.                   | Read         | -                           | -             | -     |
| coc:ticket:listEnumTypes   | Provides the permission to query the list of incident ticket enumerated types.               | List         | -                           | -             | -     |

| Action                    | Description                                                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:ticket:listEnumValues | Provides the permission to query the list of enumerated values for an incident ticket.    | List         | -                           | -             | -     |
| coc:ticket:getEnumValues  | Provides the permission to query the details of enumerated values for an incident ticket. | Read         | -                           | -             | -     |
| coc:oncall:listScenes     | Provides the permission to view on-call shift scenarios.                                  | List         | -                           | -             | -     |
| coc:oncall:createScene    | Provides the permission to create on-call shift scenarios.                                | Write        | -                           | -             | -     |
| coc:oncall:updateScene    | Provides the permission to update on-call shift scenarios.                                | Write        | -                           | -             | -     |
| coc:oncall:deleteScene    | Provides the permission to delete on-call shift scenarios.                                | Write        | -                           | -             | -     |
| coc:oncall:listRoles      | Provides the permission to query on-call shift roles.                                     | List         | -                           | -             | -     |
| coc:oncall:createRole     | Provides the permission to create on-call shift roles.                                    | Write        | -                           | -             | -     |



| Action                      | Description                                                   | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:oncall:updateRole       | Provides the permission to update on-call shift roles.        | Write        | -                           | -             | -     |
| coc:oncall:deleteRole       | Provides the permission to delete on-call shift roles.        | Write        | -                           | -             | -     |
| coc:oncall:listPersonnels   | Provides the permission to query on-call shift personnel.     | List         | -                           | -             | -     |
| coc:oncall:updatePersonnels | Provides the permission to update on-call shift personnel.    | Write        | -                           | -             | -     |
| coc:oncall:addPersonnels    | Provides the permission to add on-call shift personnel.       | Write        | -                           | -             | -     |
| coc:oncall:removePersonnels | Provides the permission to remove on-call shift personnel.    | Write        | -                           | -             | -     |
| coc:region:list             | Provides the permission to query the region list.             | List         | -                           | -             | -     |
| coc:site:list               | Provides the permission to query the site list.               | List         | -                           | -             | -     |
| coc:customApplication:list  | Provides the permission to query the custom application list. | List         | -                           | -             | -     |

| Action                       | Description                                                              | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:customApplication:get    | Provides the permission to query the details about a custom application. | Read         | -                           | -             | -     |
| coc:notificationRule:list    | Provides the permission to query the notification rule list.             | List         | -                           | -             | -     |
| coc:notificationRule:get     | Provides the permission to query notification rule details.              | Read         | -                           | -             | -     |
| coc:notificationRule:create  | Provides the permission to create a notification rule.                   | Write        | -                           | -             | -     |
| coc:notificationRule:update  | Provides the permission to update a notification rule.                   | Write        | -                           | -             | -     |
| coc:notificationRule:delete  | Provides the permission to delete a notification rule.                   | Write        | -                           | -             | -     |
| coc:notificationRule:enable  | Provides the permission to enable a notification rule.                   | Write        | -                           | -             | -     |
| coc:notificationRule:disable | Provides the permission to disable a notification rule.                  | Write        | -                           | -             | -     |
| coc:notificationRule:confirm | Provides the permission to confirm a notification rule.                  | Write        | -                           | -             | -     |

| Action                         | Description                                                      | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:notification:listTypes     | Provides the permission to query a notification type.            | List         | -                           | -             | -     |
| coc:notification:listModes     | Provides the permission to query a notification method.          | List         | -                           | -             | -     |
| coc:notification:listTemplates | Provides the permission to query the notification template list. | List         | -                           | -             | -     |
| coc:transferRule:list          | Provides the permission to query the conversion rule list.       | List         | -                           | -             | -     |
| coc:transferRule:create        | Provides the permission to create a conversion rule.             | Write        | -                           | -             | -     |
| coc:transferRule:get           | Provides the permission to query the conversion rule details.    | Read         | -                           | -             | -     |
| coc:transferRule:update        | Provides the permission to update a conversion rule.             | Write        | -                           | -             | -     |
| coc:transferRule:delete        | Provides the permission to delete a conversion rule.             | Write        | -                           | -             | -     |

| Action                        | Description                                                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:transferRule:enable       | Provides the permission to enable a conversion rule.                                | Write        | -                           | -             | -     |
| coc:transferRule:getHistory   | Provides the permission to query the messages about incidents transferred recently. | Read         | -                           | -             | -     |
| coc:transferRule:disable      | Provides the permission to disable a conversion rule.                               | Write        | -                           | -             | -     |
| coc:warroomMeetingRule:create | Provides the permission to create war room startup rules.                           | Write        | -                           | -             | -     |
| coc:warroomMeetingRule:update | Provides the permission to update war room startup rules.                           | Write        | -                           | -             | -     |
| coc:warroomMeetingRule:delete | Provides the permission to delete war room startup rules.                           | Write        | -                           | -             | -     |
| coc:warroomMeetingRule:list   | Provides the permission to query the war room startup rule list.                    | List         | -                           | -             | -     |
| coc:warroomMeetingRule:get    | Provides the permission to query the war room startup rule.                         | Read         | -                           | -             | -     |

| Action                                 | Description                                                                           | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:warroom:delete                     | Provides the permission to delete a war room.                                         | Write        | -                           | -             | -     |
| coc:warroom:getOperationHistory        | Provides the permission to query the operation history of a war room.                 | Read         | -                           | -             | -     |
| coc:warroom:addAffectedApplications    | Provides the permission to add affected applications for a war room.                  | Write        | -                           | -             | -     |
| coc:warroom:updateAffectedApplications | Provides the permission to update affected applications for a war room.               | Write        | -                           | -             | -     |
| coc:warroom:removeAffectedApplications | Provides the permission to remove affected applications from a war room.              | Write        | -                           | -             | -     |
| coc:warroom:listAffectedApplications   | Provides the permission to query the affected application list of a war room.         | List         | -                           | -             | -     |
| coc:warroom:listConfigurations         | Provides the permission to query the public enumeration configurations of a war room. | List         | -                           | -             | -     |
| coc:warroom:get                        | Provides the permission to query war room details.                                    | Read         | -                           | -             | -     |

| Action                                | Description                                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:warroom:modifyBasicInformation    | Provides the permission to modify basic war room information.             | Write        | -                           | -             | -     |
| coc:warroom:sendNotification          | Provides the permission to update or send notifications in a war room.    | Write        | -                           | -             | -     |
| coc:warroom:sendNotificationBriefing  | Provides the permission to send notification briefings in a war room.     | Write        | -                           | -             | -     |
| coc:warroom:addPersonnels             | Provides the permission to add personnel in a war room.                   | Write        | -                           | -             | -     |
| coc:warroom:removePersonnels          | Provides the permission to remove personnel from a war room.              | Write        | -                           | -             | -     |
| coc:warroom:listRoles                 | Provides the permission to query the war room role list.                  | List         | -                           | -             | -     |
| coc:warroom:addRolePersonnels         | Provides the permission to add a role to a war room.                      | Write        | -                           | -             | -     |
| coc:warroom:listNotificationTemplates | Provides the permission to query the war room notification template list. | List         | -                           | -             | -     |
| coc:warroom:listMeetings              | Provides the permission to query the war room meeting list.               | List         | -                           | -             | -     |

| Action               | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                               | Alias |
|----------------------|-----------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:schedule:count   | Provides the permission to query the number of scheduled tasks. | Read         | schedule*                   | -                                                                                                                                                           | -     |
| coc:schedule:approve | Provides the permission to review scheduled tasks.              | Write        | schedule*                   | <b>g:EnterpriseProjectId</b>                                                                                                                                | -     |
| coc:instance:stop    | Provides the permission to stop ECSs.                           | Write        | instance                    | <ul style="list-style-type: none"> <li><b>coc:ApplicationCode</b></li> <li><b>coc:ApplicationGroupCode</b></li> <li><b>g:EnterpriseProjectId</b></li> </ul> | -     |

| Action             | Description                            | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|--------------------|----------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                    |                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:instance:start | Provides the permission to start ECSs. | Write        | instance                    | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:ApplicationGroupCode</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                | -     |



| Action              | Description                              | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|---------------------|------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                     |                                          |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:instance:reboot | Provides the permission to restart ECSs. | Write        | instance                    | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:ApplicationGroupCode</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                | -     |

| Action            | Description                                                 | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|-------------------|-------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                   |                                                             |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:appkey:create | Provides the permission to create a mobile application key. | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:appkey:delete | Provides the permission to delete a mobile application key. | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:appkey:get    | Provides the permission to view a mobile application key.   | Read         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |

| Action                                 | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                  | Alias |
|----------------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:appkey:update                      | Provides the permission to update a mobile application key.         | Write        | -                           | -                                                                                                                              | -     |
| coc:failureMode:create                 | Provides the permission to create a failure mode.                   | Write        | failure Mode *              | -                                                                                                                              | -     |
| coc:failureMode:update                 | Provides the permission to update a failure mode.                   | Write        | failure Mode *              | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul> | -     |
| coc:failureMode:get                    | Provides the permission to query details of a failure mode.         | Read         | failure Mode *              | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul> | -     |
| coc:failureMode:delete                 | Provides the permission to delete a failure mode.                   | Write        | failure Mode *              | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul> | -     |
| coc:failureMode:list                   | Provides the permission to query the failure mode list.             | List         | failure Mode *              | -                                                                                                                              | -     |
| coc:application:CreateResourceTopology | Provides the permission to create an application resource topology. | Write        | application *               | -                                                                                                                              | -     |
| coc:application:GetResourceTopology    | Provides the permission to view an application resource topology.   | Read         | application *               | -                                                                                                                              | -     |

| Action                                  | Description                                                               | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                  | Alias |
|-----------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:application:CreateDiagnosisTask     | Provides the permission to create an application resource diagnosis task. | Write        | application *               | -                                                                                                                              | -     |
| coc:application:GetDiagnosisTaskDetails | Provides the permission to query application resource diagnosis tasks.    | Read         | application *               | -                                                                                                                              | -     |
| coc:contingencyPlan:create              | Provides the permission to create contingency plans.                      | Write        | contingencyPlan *           | -                                                                                                                              | -     |
| coc:contingencyPlan:get                 | Provides the permission to query contingency plan details.                | Read         | contingencyPlan *           | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul> | -     |
| coc:contingencyPlan:update              | Provides the permission to modify contingency plans.                      | Write        | contingencyPlan *           | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul> | -     |
| coc:contingencyPlan:delete              | Provides the permission to delete contingency plans.                      | Write        | contingencyPlan *           | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul> | -     |
| coc:contingencyPlan:list                | Provides the permission to query contingency plans.                       | List         | contingencyPlan *           | -                                                                                                                              | -     |

| Action                              | Description                                                                       | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                           | Alias |
|-------------------------------------|-----------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:contingencyPlan:uploadFile      | Provides the permission to upload attachments to contingency plans.               | Write        | -                           | -                                                                                                                                       | -     |
| coc:contingencyPlan:downloadFile    | Provides the permission to download attachments from contingency plans.           | Read         | contingencyPlan *           | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul>          | -     |
| coc:attackTask:create               | Provides the permission to create an attack task.                                 | Write        | attackTask *                | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:AttackTargetType</a></li> </ul> | -     |
| coc:attackTask:get                  | Provides the permission to view attack task details.                              | Read         | attackTask *                | <ul style="list-style-type: none"> <li>• <a href="#">coc:ApplicationCode</a></li> <li>• <a href="#">coc:Creator</a></li> </ul>          | -     |
| coc:attackTask:list                 | Provides the permission to view the attack task list.                             | List         | attackTask *                | -                                                                                                                                       | -     |
| coc:attackTask:deleteRelatedRecords | Provides the permission to delete attack task records.                            | Write        | attackTask *                | -                                                                                                                                       | -     |
| coc:attackRecord:list               | Provides the permission to view the attack record list.                           | List         | attackRecord *              | -                                                                                                                                       | -     |
| coc:attackTargetRecord:list         | Provides the permission to view the execution record list of a disruption target. | List         | attackTargetRecord *        | -                                                                                                                                       | -     |

| Action                             | Description                                                              | Access Level | Resource Type (*: Required) | Condition Key                                                                                            | Alias |
|------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------|-------|
| coc:attackTargetRecord:operate     | Provides the permission to retry execution records of disruption target. | Write        | attackTargetRecord *        | <b>coc:Creator</b>                                                                                       | -     |
| coc:drillTask:create               | Provides the permission to create a drill task.                          | Write        | drillTask *                 | <b>coc:ApplicationCode</b>                                                                               | -     |
| coc:drillTask:update               | Provides the permission to modify a drill task.                          | Write        | drillTask *                 | <ul style="list-style-type: none"> <li><b>coc:ApplicationCode</b></li> <li><b>coc:Creator</b></li> </ul> | -     |
| coc:drillTask:list                 | Provides the permission to view the drill task list.                     | List         | drillTask *                 | -                                                                                                        | -     |
| coc:drillTask:get                  | Provides the permission to query drill task details.                     | Read         | drillTask *                 | <b>coc:Creator</b>                                                                                       | -     |
| coc:drillTask:delete               | Provides the permission to delete drill tasks.                           | Write        | drillTask *                 | <b>coc:Creator</b>                                                                                       | -     |
| coc:drillTask:deleteRelatedRecords | Provides the permission to delete drill task records.                    | Write        | drillTask *                 | -                                                                                                        | -     |
| coc:drillRecord:create             | Provides the permission to start a drill.                                | Write        | drillRecord *               | <b>coc:Creator</b>                                                                                       | -     |

| Action                 | Description                                            | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|------------------------|--------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                        |                                                        |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:drillRecord:get    | Provides the permission to query drill record details. | Read         | drill Record *              | <a href="#">coc:Creator</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | -     |
| coc:drillReport:create | Provides the permission to create a drill report.      | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:drillReport:update | Provides the permission to update a drill report.      | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |

| Action                     | Description                                                   | Access Level | Resource Type (*: Required) | Condition Key                                                                                                           | Alias |
|----------------------------|---------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------|-------|
| coc:drillReport:get        | Provides the permission to query drill report details.        | Read         | -                           | -                                                                                                                       | -     |
| coc:improvementTask:create | Provides the permission to create improvement items.          | Write        | -                           | -                                                                                                                       | -     |
| coc:improvementTask:update | Provides the permission to handle improvement items.          | Write        | -                           | -                                                                                                                       | -     |
| coc:improvementTask:list   | Provides the permission to query improvement items.           | List         | -                           | -                                                                                                                       | -     |
| coc:improvementTask:get    | Provides the permission to query improvement item details.    | Read         | -                           | -                                                                                                                       | -     |
| coc:drillPlan:create       | Provides the permission to create a drill plan.               | Write        | -                           | -                                                                                                                       | -     |
| coc:drillPlan:update       | Provides the permission to update a drill plan.               | Write        | drill Plan *                | <ul style="list-style-type: none"> <li>• <a href="#">coc:Creator</a></li> <li>• <a href="#">coc:Executor</a></li> </ul> | -     |
| coc:drillPlan:get          | Provides the permission to query the details of a drill plan. | Read         | drill Plan *                | <ul style="list-style-type: none"> <li>• <a href="#">coc:Creator</a></li> <li>• <a href="#">coc:Executor</a></li> </ul> | -     |



| Action                             | Description                                                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:drillPlan:list                 | Provides the permission to query the drill plan list.                                      | List         | -                           | -             | -     |
| coc:drillPlan:listDelay            | Provides the permission to query the drill plan extension list.                            | List         | -                           | -             | -     |
| coc:drillPlan:countStatus          | Provides the permission to query the number of drill plans in a specified status.          | Read         | -                           | -             | -     |
| coc:drillPlan:countDelay           | Provides the permission to query the number of postponed drills of a specified drill plan. | Read         | -                           | -             | -     |
| coc:attackTarget:listCceNamespaces | Provides the permission to query the namespace list of CCE disruption targets.             | List         | -                           | -             | -     |
| coc:attackTarget:listCceWorkloads  | Provides the permission to query the workload list of CCE attack targets.                  | List         | -                           | -             | -     |
| coc:attackTarget:listCcePods       | Provides the permission to query the pod list of CCE disruption targets.                   | List         | -                           | -             | -     |

| Action                            | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias               |
|-----------------------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------|
| coc:monitorMetric:list            | Provides the permission to query the monitoring metric list.        | List         | -                           | -             | -                   |
| coc:monitorMetricRecord:list      | Provides the permission to query the monitoring metric data list.   | List         | -                           | -             | -                   |
| coc:attackRecord:changeMetricType | Provides the permission to modify metric types in an attack record. | Write        | attackRecord *              | -             | -                   |
| coc:prTemplate:create             | Provides the permission to create a PRR template.                   | Write        | -                           | -             | -                   |
| coc:prTemplate:update             | Provides the permission to modify a PRR template.                   | Write        | -                           | -             | -                   |
| coc:prTemplate:list               | Provides the permission to view a PRR template list.                | List         | -                           | -             | -                   |
| coc:prTemplate:get                | Provides the permission to query a PRR template details.            | Read         | -                           | -             | -                   |
| coc:prTemplate:delete             | Provides the permission to delete a PRR template.                   | Write        | -                           | -             | -                   |
| coc::listPrrCheckItem             | Provides the permission to view a PRR check item list.              | List         | -                           | -             | coc:prTemplate:list |

| Action                          | Description                                                       | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:prReview:create             | Provides the permission to start a PRR review.                    | Write        | -                           | -             | -     |
| coc:prReview:update             | Provides the permission to continue to start a PRR review.        | Write        | -                           | -             | -     |
| coc:prReview:list               | Provides the permission to view a PRR review list.                | List         | -                           | -             | -     |
| coc:prReview:get                | Provides the permission to query a PRR review details.            | Read         | -                           | -             | -     |
| coc:prReview:recordSummary      | Provides the permission to input PRR review minutes.              | Write        | -                           | -             | -     |
| coc:prReview:auditResult        | Provides the permission to input PRR review conclusions.          | Write        | -                           | -             | -     |
| coc:prReview:delete             | Provides the permission to cancel a PRR review.                   | Write        | -                           | -             | -     |
| coc:prReview:addImprovementTask | Provides the permission to add PRR improvement items.             | Write        | -                           | -             | -     |
| coc:instance:listAlarms         | Provides the permission to query the alarm list of all resources. | List         | -                           | -             | -     |

| Action                  | Description                                                   | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:instance:get Alarms | Provides the permission to view the alarm list of a resource. | Read         | -                           | -             | -     |
| coc:alarm:list          | Provides the permission to query the alarm list.              | List         | -                           | -             | -     |
| coc:alarm:count         | Provides the permission to query the number of alarms.        | Read         | -                           | -             | -     |
| coc:slaTemplate:list    | Provides the permission to query the SLA template list.       | List         | slaTemplate *               | -             | -     |
| coc:slaTemplate:get     | Provides the permission to query SLA template details.        | Read         | slaTemplate *               | -             | -     |
| coc:slaTemplate:create  | Provides the permission to create an SLA template.            | Write        | slaTemplate *               | -             | -     |
| coc:slaTemplate:delete  | Provides the permission to delete an SLA template.            | Write        | slaTemplate *               | -             | -     |
| coc:slaTemplate:enable  | Provides the permission to enable an SLA template.            | Write        | slaTemplate *               | -             | -     |
| coc:slaTemplate:disable | Provides the permission to disable an SLA template.           | Write        | slaTemplate *               | -             | -     |

| Action                     | Description                                                         | Access Level | Resource Type (*: Required) | Condition Key      | Alias |
|----------------------------|---------------------------------------------------------------------|--------------|-----------------------------|--------------------|-------|
| coc:slaTemplate:update     | Provides the permission to modify an SLA template.                  | Write        | slaTemplate *               | -                  | -     |
| coc:slaRecord:list         | Provides the permission to query the SLA service ticket list.       | List         | -                           | -                  | -     |
| coc:slaRecord:get          | Provides the permission to query the SLA service ticket details.    | Read         | -                           | -                  | -     |
| coc:customDashboard:get    | Provides the permission to query the custom dashboard.              | Read         | -                           | -                  | -     |
| coc:customDashboard:update | Provides the permission to modify the custom dashboard.             | Write        | -                           | -                  | -     |
| coc:agency:get             | Provides the permission to query agency information about a tenant. | Read         | -                           | -                  | -     |
| coc:agency:create          | Provides the permission to create a tenant agency.                  | Write        | -                           | -                  | -     |
| coc:parameter:create       | Provides the permission to create a parameter.                      | Write        | parameter *                 | <b>coc:Creator</b> | -     |
| coc:parameter:update       | Provides the permission to update a parameter.                      | Write        | parameter *                 | <b>coc:Creator</b> | -     |

| Action                     | Description                                            | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Alias |
|----------------------------|--------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:parameter:get          | Provides the permission to query parameter details.    | Read         | parameter *                 | <b>coc:Creator</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                               | -     |
| coc:parameter:delete       | Provides the permission to delete parameters.          | Write        | parameter *                 | <b>coc:Creator</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                               | -     |
| coc:parameter:list         | Provides the permission to query the parameter list.   | List         | parameter *                 | <b>coc:Creator</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                               | -     |
| coc:accountBaseline:create | Provides the permission to create an account baseline. | Write        | accountBaseline *           | <ul style="list-style-type: none"> <li><b>coc:Ticket Level</b></li> <li><b>coc:Ticket Scope</b></li> <li><b>coc:RequestScope</b></li> <li><b>coc:Ticket CurrentHandlers</b></li> <li><b>coc:Ticket Status</b></li> <li><b>coc:Ticket Type</b></li> <li><b>coc:Ticket BeginTime</b></li> <li><b>coc:Ticket EndTime</b></li> <li><b>coc:RequestTarget</b></li> <li><b>coc:Ticket Target</b></li> <li><b>coc:OperatorName</b></li> <li><b>coc:Escape SwitchIsEnabled</b></li> </ul> | -     |

| Action                              | Description                                                        | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|-------------------------------------|--------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:accountBaseline:list            | Provides the permission to query the account baseline list.        | List         | accountBaseline *           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:accountBaseline:listAccountList | Provides the permission to query the account list in the baseline. | List         | accountBaseline *           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:accountBaseline:deleteAccount   | Provides the permission to delete accounts from a baseline.        | Write        | accountBaseline *           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:accountBaseline:update          | Provides the permission to modify account baselines.               | Write        | accountBaseline *           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> | -     |

| Action                                | Description                                                              | Access Level | Resource Type (*: Required) | Condition Key                         | Alias |
|---------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| coc:accountBaseline:delete            | Provides the permission to delete account baselines.                     | Write        | accountBaseline *           | -                                     | -     |
| coc:instance:getAccount               | Provides the permission to query the list of managed accounts on a host. | List         | instance                    | -                                     | -     |
| coc:instance:syncAccount              | Provides the permission to synchronize accounts of hosts.                | Write        | instance *                  | <a href="#">g:EnterpriseProjectId</a> | -     |
| coc:instance:resetPassword            | Provides the permission to reset the password of a host account.         | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| coc:instance:resetAccountPassword     | Provides the permission to reset the password of a host account.         | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| coc:instance:createPasswordChangePlan | Provides the permission to create a password change plan.                | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| coc:instance:updateAccountPassword    | Provides the permission to write back the password change result.        | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -     |
| coc:instance:addAccount               | Provides the permission to import accounts of hosts.                     | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | -     |



| Action                             | Description                                                              | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Alias |
|------------------------------------|--------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| coc:instance:getAccountPassword    | Provides the permission to query the account and password of a host.     | Read         | instance                    | <b>g:EnterpriseProjectId</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | -     |
|                                    |                                                                          |              | -                           | <ul style="list-style-type: none"> <li>• <b>coc:TicketLevel</b></li> <li>• <b>coc:TicketScope</b></li> <li>• <b>coc:RequestScope</b></li> <li>• <b>coc:TicketCurrentHandlers</b></li> <li>• <b>coc:TicketStatus</b></li> <li>• <b>coc:TicketType</b></li> <li>• <b>coc:TicketBeginTime</b></li> <li>• <b>coc:TicketEndTime</b></li> <li>• <b>coc:RequestTarget</b></li> <li>• <b>coc:TicketTarget</b></li> <li>• <b>coc:OperatorName</b></li> <li>• <b>coc:EscapeSwitchIsEnabled</b></li> </ul> |       |
| coc:instance:getHistoricalPassword | Provides the permission to query historical passwords of a host account. | Read         | instance                    | <b>g:EnterpriseProjectId</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | -     |

| Action                                | Description                                                                     | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias                        |
|---------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
|                                       |                                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |                              |
| coc:instance:getPasswordChangeRecords | Provides the permission to query the password change records of a host account. | Read         | instance                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -                            |
| coc::getAccountManagedStatus          | Provides the permission to query the management step status.                    | Read         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | coc:account:getManagedStatus |

| Action                             | Description                                                                                              | Access Level | Resource Type (*: Required) | Condition Key | Alias                                     |
|------------------------------------|----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------------|
| coc::addAutoManagementRelations    | Provides the permission to enable automatic management by component.                                     | Write        | -                           | -             | coc:accountAutoManagement:addRelations    |
| coc::getAutoManagementRelations    | Provides the permission to query information about components for which automatic management is enabled. | List         | -                           | -             | coc:accountAutoManagement:getRelations    |
| coc::deleteAutoManagementRelations | Provides the permission to disable automatic management by component.                                    | Write        | -                           | -             | coc:accountAutoManagement:deleteRelations |
| coc::getAutoManagementStatus       | Provides the permission to query whether the automatic management function is enabled.                   | Read         | -                           | -             | coc:accountAutoManagement:getStatus       |
| coc::updateAutoManagementStatus    | Provides the permission to update the automatic management status.                                       | Write        | -                           | -             | coc:accountAutoManagement:updateStatus    |
| coc::addEncryptionKey              | Provides the permission to add an encryption key.                                                        | Write        | -                           | -             | coc:accountEncryptionKey:add              |

| Action                          | Description                                            | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias                                  |
|---------------------------------|--------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| coc::listDEWKeys                | Provides the permission to query existing DEW keys.    | List         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | coc:accountEncryptionKey:listDEWKeys   |
| coc::listEncryptionKey          | Provides the permission to query added DEW keys.       | List         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | coc:accountEncryptionKey:list          |
| coc::enablePasswordChangePolicy | Provides the permission to enable a key change policy. | Write        | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> | coc:accountPasswordChangePolicy:enable |

| Action                       | Description                                                          | Access Level | Resource Type (*: Required) | Condition Key         | Alias                               |
|------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|-----------------------|-------------------------------------|
| coc::getPasswordChangePolicy | Provides the permission to query enabled password change policies.   | List         | -                           | -                     | coc:accountPasswordChangePolicy:get |
| coc:incident:create          | Provides the permission to create incident tickets using COC.        | Write        | -                           | -                     | -                                   |
| coc:incident:handle          | Provides the permission to handle incident tickets using COC.        | Write        | -                           | -                     | -                                   |
| coc:incident:detail          | Provides the permission to obtain incident ticket details using COC. | Read         | -                           | -                     | -                                   |
| coc:session:start            | Provides the permission to log in to an ECS without a password.      | Write        | instance                    | g:EnterpriseProjectId | -                                   |

| Action                           | Description                                             | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias                                   |
|----------------------------------|---------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
|                                  |                                                         |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |                                         |
| coc::disablePasswordChangePolicy | Provides the permission to disable a key change policy. | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | coc:accountPasswordChangePolicy:disable |
| coc::createOrders                | Provides the permission to create COC orders.           | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | coc:orders:create                       |

| Action                                               | Description                                                    | Access Level | Resource Type (*: Required) | Condition Key                | Alias             |
|------------------------------------------------------|----------------------------------------------------------------|--------------|-----------------------------|------------------------------|-------------------|
| coc::changeOrders                                    | Provides the permission to update COC orders.                  | Write        | -                           | -                            | coc:orders:change |
| coc::listQuotas                                      | Provides the permission to query the list of purchased quotas. | List         | -                           | -                            | coc:quotas:list   |
| coc:alarm:put                                        | Provides the permission to report COC alarms.                  | Write        | -                           | -                            | -                 |
| coc:application:AddComponentInvokingRelationships    | Provides the permission to create component relationships.     | Write        | application *               | -                            | -                 |
| coc:application:RemoveComponentInvokingRelationships | Provides the permission to delete component connections.       | Write        | application *               | -                            | -                 |
| coc:application:ListComponentInvokingRelationships   | Provides the permission to view component connections.         | Read         | application *               | -                            | -                 |
| coc:instance:updateResources                         | Provides the permission to update resource information.        | Write        | -                           | -                            | -                 |
| coc:instance:restartRDSInstance                      | Provides the permission to reboot an RDS DB instance.          | Write        | instance                    | <b>g:EnterpriseProjectId</b> | -                 |

| Action                        | Description                                           | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|-------------------------------|-------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                               |                                                       |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:instance:startRDSInstance | Provides the permission to enable an RDS DB instance. | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -     |



| Action                       | Description                                         | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|------------------------------|-----------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                              |                                                     |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:instance:stopRDSInstance | Provides the permission to stop an RDS DB instance. | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | -     |

| Action                  | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Alias |
|-------------------------|-----------------------------------------------------------------|--------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                         |                                                                 |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">coc:TicketLevel</a></li> <li>• <a href="#">coc:TicketScope</a></li> <li>• <a href="#">coc:RequestScope</a></li> <li>• <a href="#">coc:TicketCurrentHandlers</a></li> <li>• <a href="#">coc:TicketStatus</a></li> <li>• <a href="#">coc:TicketType</a></li> <li>• <a href="#">coc:TicketBeginTime</a></li> <li>• <a href="#">coc:TicketEndTime</a></li> <li>• <a href="#">coc:RequestTarget</a></li> <li>• <a href="#">coc:TicketTarget</a></li> <li>• <a href="#">coc:OperatorName</a></li> <li>• <a href="#">coc:EscapeSwitchIsEnabled</a></li> </ul> |       |
| coc:systemConfig:create | Provides the permission to create a system configuration.       | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:systemConfig:list   | Provides the permission to query the system configuration list. | List         | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |
| coc:systemConfig:update | Provides the permission to update system configurations.        | Write        | -                           | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | -     |

| Action                   | Description                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:systemConfig:get     | Provides the permission to display system configurations. | Read         | -                           | -             | -     |
| coc:hostAccount:add      | Provides the permission to add a hosting account.         | Write        | -                           | -             | -     |
| coc:hostAccount:list     | Provides the permission to query SRE hosting accounts.    | List         | -                           | -             | -     |
| coc:hostAccount:update   | Provides the permission to edit SRE hosting accounts.     | Write        | -                           | -             | -     |
| coc:hostAccount:delete   | Provides the permission to delete SRE hosting accounts.   | Write        | -                           | -             | -     |
| coc:hostAccount:describe | Grant an account to view its hosting account information. | Read         | -                           | -             | -     |
| coc:hostAccount:enable   | Grant an account to enable the hosting service.           | Write        | -                           | -             | -     |
| coc:hostAccount:disable  | Grant an account to disable the hosting service.          | Write        | -                           | -             | -     |
| coc:slo:list             | Provides the permission to query the SLO list.            | List         | -                           | -             | -     |
| coc:slo:createSloTarget  | Provides the permission to create an SLO.                 | Write        | -                           | -             | -     |

| Action                                    | Description                                                                      | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:slo:deleteSloTarget                   | Provides the permission to delete an SLO.                                        | Write        | -                           | -             | -     |
| coc:slo:updateSloTarget                   | Provides the permission to update an SLO.                                        | Write        | -                           | -             | -     |
| coc:slo:getSloDetail                      | Provides the permission to query an SLO.                                         | Read         | -                           | -             | -     |
| coc:slo:listSli                           | Provides the permission to query the SLI list.                                   | List         | -                           | -             | -     |
| coc:slo:configureSli                      | Provides the permission to update the SLI list.                                  | Write        | -                           | -             | -     |
| coc:slo:createInterruptRecords            | Provides the permission to create SLO interruption records.                      | Write        | -                           | -             | -     |
| coc:slo:listInterruptRecords              | Provides the permission to query SLO interruption records.                       | List         | -                           | -             | -     |
| coc:slo:updateInterruptRecords            | Provides the permission to update SLO interruption records.                      | Write        | -                           | -             | -     |
| coc:slo:listInterruptRecordsChangeHistory | Provides the permission to query the change history of SLO interruption records. | List         | -                           | -             | -     |

| Action                              | Description                                                                                                   | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:crossAccounts:authorize         | Provides the permission to authorize cross-account management.                                                | Write        | -                           | -             | -     |
| coc:crossAccounts:listCrossAccounts | Provides the permission to query information about your own account in the cross-account management scenario. | List         | -                           | -             | -     |
| coc:alarmRule:list                  | Provides the permission to query alarm rules.                                                                 | List         | -                           | -             | -     |
| coc:alarmRule:sync                  | Provides the permission to synchronize alarm rules.                                                           | Write        | -                           | -             | -     |
| coc:alarmRule:put                   | Provides the permission to enable or disable alarm rules.                                                     | Write        | -                           | -             | -     |
| coc:alarmRule:delete                | Provides the permission to delete an alarm rule.                                                              | Write        | -                           | -             | -     |
| coc:ticket:updateEnumValues         | Provides the permission to update a child enumerated value.                                                   | Write        | -                           | -             | -     |
| coc:ticket:createEnumValues         | Provides the permission to create a child enumerated value.                                                   | Write        | -                           | -             | -     |

| Action                                 | Description                                                                                | Access Level | Resource Type (*: Required) | Condition Key                      | Alias                        |
|----------------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------------|------------------------------|
| coc:ticket:deleteEnumValues            | Provides the permission to delete a child enumerated value.                                | Write        | -                           | -                                  | -                            |
| coc:integration:create                 | Provides the permission to create integration configurations.                              | Write        | -                           | -                                  | -                            |
| coc:integration:downloadZabbixTemplate | Provides the permission to download the Zabbix template of an alarm source.                | Read         | -                           | -                                  | -                            |
| coc:quickSetupConfigurations:create    | Provides the permission to quickly configure global cloud service configuration scenarios. | Write        | -                           | <a href="#">coc:QuickSetupType</a> | -                            |
| coc::updateServiceConfigTask           | Provides the permission to modify cloud service configuration tasks.                       | Write        | -                           | -                                  | coc:serviceConfigTask:update |
| coc::listServiceConfigTask             | Provides the permission to query cloud service configuration tasks.                        | List         | -                           | -                                  | coc:serviceConfigTask:list   |
| coc:instance:deleteResourceTags        | Provides the permission to delete resource tags.                                           | Write        | -                           | -                                  | -                            |

| Action                         | Description                                                           | Access Level | Resource Type (*: Required) | Condition Key                       | Alias                          |
|--------------------------------|-----------------------------------------------------------------------|--------------|-----------------------------|-------------------------------------|--------------------------------|
| coc::getBiSubscription         | Provides the permission to query the BI subscription records.         | Read         | -                           | -                                   | coc:biSubscription:get         |
| coc::listBiSubscription        | Provides the permission to query the BI subscription record list.     | List         | -                           | -                                   | coc:biSubscription:list        |
| coc::listBiSubscriptionHistory | Provides the permission to query the BI subscription history records. | List         | -                           | -                                   | coc:biSubscriptionHistory:list |
| coc::createBiSubscription      | Provides the permission to create BI subscription records.            | Write        | -                           | -                                   | coc:biSubscription:create      |
| coc::deleteBiSubscription      | Provides the permission to delete BI subscription records.            | Write        | -                           | -                                   | coc:biSubscription:delete      |
| coc::updateBiSubscription      | Provides the permission to update BI subscription records.            | Write        | -                           | -                                   | coc:biSubscription:update      |
| coc:assessTask:list            | Provides the permission to query the evaluation task list.            | List         | -                           | -                                   | -                              |
| coc:assessTask:create          | Provides the permission to create an evaluation task.                 | Write        | -                           | <a href="#">coc:ApplicationCode</a> | -                              |

| Action                            | Description                                                                           | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------|---------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:assessTask:delete             | Provides the permission to delete an evaluation task.                                 | Write        | -                           | -             | -     |
| coc:assessTask:countByStatus      | Provides the permission to query the number of evaluation tasks by status.            | Read         | -                           | -             | -     |
| coc:assessTask:countReports       | Provides the permission to view the number of evaluation reports of evaluation tasks. | Read         | -                           | -             | -     |
| coc:assessTask:countDistributions | Provides the permission to view the distribution of evaluation tasks.                 | Read         | -                           | -             | -     |
| coc:assessReport:delete           | Provides the permission to delete an evaluation report.                               | Write        | -                           | -             | -     |
| coc:assessReport:create           | Provides the permission to create an evaluation report.                               | Write        | -                           | -             | -     |
| coc:assessReport:get              | Provides the permission to query evaluation report details.                           | Read         | -                           | -             | -     |
| coc:assessReport:updateItemStatus | Provides the permission to modify the evaluation item status of an evaluation report. | Write        | -                           | -             | -     |



| Action                   | Description                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|--------------------------|-----------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:assessReport:list    | Provides the permission to query evaluation reports.      | List         | -                           | -             | -     |
| coc:product:list         | Provides the permission to query the product list.        | List         | -                           | -             | -     |
| coc:product:get          | Grants end users the permission to query product details. | Read         | product *                   | -             | -     |
| coc:product:search       | Provides the permission to query the product list.        | List         | -                           | -             | -     |
| coc:product:show         | Provides the permission to query product details.         | Read         | product *                   | -             | -     |
| coc:product:create       | Provides the permission to create a product.              | Write        | product *                   | -             | -     |
| coc:product:update       | Provides the permission to update a product.              | Write        | product *                   | -             | -     |
| coc:product:delete       | Provides the permission to delete a product.              | Write        | product *                   | -             | -     |
| coc:product:listVersions | Provides the permission to query product versions.        | List         | -                           | -             | -     |
| coc:product:getVersion   | Provides the permission to query product version details. | Read         | product *                   | -             | -     |

| Action                    | Description                                                      | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|---------------------------|------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:product:createVersion | Provides the permission to create a product version.             | Write        | product *                   | -             | -     |
| coc:product:updateVersion | Provides the permission to update a product version.             | Write        | product *                   | -             | -     |
| coc:product:deleteVersion | Provides the permission to delete a product version.             | Write        | product *                   | -             | -     |
| coc:portfolio:search      | Provides the permission to query the list of product portfolios. | List         | -                           | -             | -     |
| coc:portfolio:show        | Provides the permission to query product portfolio details.      | Read         | portfolio *                 | -             | -     |
| coc:portfolio:create      | Provides the permission to create a product portfolio.           | Write        | portfolio *                 | -             | -     |
| coc:portfolio:update      | Provides the permission to update a product portfolio.           | Write        | portfolio *                 | -             | -     |
| coc:portfolio:delete      | Provides the permission to delete a product portfolio.           | Write        | portfolio *                 | -             | -     |

| Action                                   | Description                                                                                 | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------------|---------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:portfolio:searchProductsForPortfolio | Provides the permission to query the relationship between a product portfolio and products. | List         | -                           | -             | -     |
| coc:portfolio:associateProduct           | Provides the permission to create relationships between product portfolios and products.    | Write        | portfolio *                 | -             | -     |
| coc:portfolio:disassociateProduct        | Provides the permission to delete relationships between product portfolios and products.    | Write        | portfolio *                 | -             | -     |
| coc:portfolio:searchPrincipals           | Provides the permission to query product portfolio authorization lists.                     | List         | -                           | -             | -     |
| coc:portfolio:associatePrincipal         | Provides the permission to associate a principal with a product portfolio.                  | Write        | portfolio *                 | -             | -     |
| coc:portfolio:disassociatePrincipal      | Provides the permission to disassociate a principal from a portfolio.                       | Write        | portfolio *                 | -             | -     |

| Action                               | Description                                                                        | Access Level | Resource Type (*: Required) | Condition Key | Alias                                  |
|--------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------|
| coc:provisionedProduct:list          | Provides the permission to query product instances.                                | List         | -                           | -             | -                                      |
| coc:provisionedProduct:get           | Provides the permission to query product instance details.                         | Read         | provisionedProduct *        | -             | -                                      |
| coc:provisionedProduct:listEvents    | Provides the permission to query an incident resource stack of a product instance. | List         | provisionedProduct *        | -             | -                                      |
| coc:provisionedProduct:listResources | Provides the permission to query product instance resource stack resources.        | List         | provisionedProduct *        | -             | -                                      |
| coc:provisionedProduct:create        | Provides the permission to create a product instance.                              | Write        | provisionedProduct *        | -             | -                                      |
| coc:provisionedProduct:delete        | Provides the permission to delete a product instance.                              | Write        | provisionedProduct *        | -             | -                                      |
| coc::getServiceCatalogRole           | Provides the permission to verify a service catalog user role.                     | Read         | -                           | -             | coc:system:getServiceCatalogRole       |
| coc::listQuickSetupConfiguration     | Provides the permission to quickly obtain the configuration task list.             | List         | -                           | -             | coc:system:listQuickSetupConfiguration |

| Action                                | Description                                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias                                       |
|---------------------------------------|---------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------|
| coc::getQuickSetupConfiguration       | Provides the permission to quickly obtain the configuration task details. | Read         | -                           | -             | coc:system:getQuickSetupConfiguration       |
| coc::createQuickSetupConfiguration    | Provides the permission to quickly create configuration tasks.            | Write        | -                           | -             | coc:system:createQuickSetupConfiguration    |
| coc::listQuickSetupConfigurationTasks | Provides the permission to quickly obtain the subtask list of a task.     | List         | -                           | -             | coc:system:listQuickSetupConfigurationTasks |
| coc::createNotificationGroup          | Provides the permission to add a notification group.                      | Write        | -                           | -             | coc:system:createNotificationGroup          |
| coc::updateNotificationGroup          | Provides the permission to update a notification group.                   | Write        | -                           | -             | coc:system:updateNotificationGroup          |
| coc::deleteNotificationGroup          | Provides the permission to delete a notification group.                   | Write        | -                           | -             | coc:system:deleteNotificationGroup          |
| coc::listNotificationGroup            | Provides the permission to query a notification group.                    | List         | -                           | -             | coc:system:listNotificationGroup            |

| Action                          | Description                                                                                                  | Access Level | Resource Type (*: Required) | Condition Key | Alias                                 |
|---------------------------------|--------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------|
| coc::subscribeNotificationGroup | Provides the permission to subscribe to a notification group.                                                | Write        | -                           | -             | coc:system:subscribeNotificationGroup |
| coc:product:createConstraint    | Provides the permission to create a constraint.                                                              | Write        | product *                   | -             | coc:system:subscribeNotificationGroup |
| coc:product:deleteConstraint    | Provides the permission to delete a constraint.                                                              | Write        | product *                   | -             | coc:system:subscribeNotificationGroup |
| coc:product:updateConstraint    | Provides the permission to update a constraint.                                                              | Write        | product *                   | -             | coc:system:subscribeNotificationGroup |
| coc:product:getConstraint       | Provides the permission to query constraint details.                                                         | Read         | product *                   | -             | coc:system:subscribeNotificationGroup |
| coc:product:listConstraint      | Provides the permission to query the constraint list.                                                        | List         | -                           | -             | -                                     |
| coc::getOSUpgradePath           | Provides the permission to determine the upgrade configuration information based on the tenant upgrade path. | Read         | -                           | -             | coc:system:getOSUpgradePath           |

| Action                                 | Description                                                                                                                          | Access Level | Resource Type (*: Required) | Condition Key                         | Alias                                        |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------------------------|
| coc::getOSCustomScriptRuntimeParams    | Provides the permission to obtain the custom script configuration information set by the tenant in the OS upgrade and rollback jobs. | Read         | -                           | -                                     | coc:system:getOSCustomScriptRuntimeParams    |
| coc::updateOSCustomScriptRuntimeParams | Provides the permission to modify the custom script configuration information set by the tenant in the OS upgrade and rollback jobs. | Write        | -                           | -                                     | coc:system:updateOSCustomScriptRuntimeParams |
| coc:vm:upgradeOsVersion                | Provides the permission to upgrade an OS version.                                                                                    | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | coc:system:updateOSCustomScriptRuntimeParams |
|                                        |                                                                                                                                      |              | vm                          | -                                     |                                              |
| coc:vm:rollbackOsVersion               | Provides the permission to roll back an OS version.                                                                                  | Write        | instance                    | <a href="#">g:EnterpriseProjectId</a> | coc:system:updateOSCustomScriptRuntimeParams |
|                                        |                                                                                                                                      |              | vm                          | -                                     |                                              |
| coc:sloBasicData:list                  | Provides the permission to query the basic data list.                                                                                | List         | -                           | -                                     | -                                            |
| coc:sloBasicData:create                | Provides the permission to add basic data.                                                                                           | Write        | -                           | -                                     | -                                            |

| Action                    | Description                                                  | Access Level | Resource Type (*: Required) | Condition Key                                                                                                                    | Alias                           |
|---------------------------|--------------------------------------------------------------|--------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| coc:sloBasicData:update   | Provides the permission to modify basic data.                | Write        | -                           | -                                                                                                                                | -                               |
| coc:sloBasicData:delete   | Provides the permission to delete basic data.                | Write        | -                           | -                                                                                                                                | -                               |
| coc:sloDiagram:get        | Provides the permission to query diagram details.            | Read         | sloDiagram *                | <ul style="list-style-type: none"> <li>• <a href="#">coc:Creator</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                               |
| coc:sloDiagram:create     | Provides the permission to create a diagram.                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>                                                                                            | -                               |
| coc:sloDiagram:list       | Provides the permission to query diagram lists.              | List         | -                           | -                                                                                                                                | -                               |
| coc:sloDiagram:update     | Provides the permission to modify diagrams.                  | Write        | sloDiagram *                | <ul style="list-style-type: none"> <li>• <a href="#">coc:Creator</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                               |
| coc:sloDiagram:delete     | Provides the permission to delete diagrams.                  | Write        | sloDiagram *                | <ul style="list-style-type: none"> <li>• <a href="#">coc:Creator</a></li> <li>• <a href="#">g:EnterpriseProjectId</a></li> </ul> | -                               |
| coc::getTopology          | Provides the permission to query topology details.           | Read         | -                           | -                                                                                                                                | coc:system:getTopology          |
| coc::getTopologyDimension | Provides the permission to query topology dimension details. | Read         | -                           | -                                                                                                                                | coc:system:getTopologyDimension |



| Action                                  | Description                                                                                                    | Access Level | Resource Type (*: Required) | Condition Key | Alias                                         |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------------|
| coc::getTopologyVertexDetails           | Provides the permission to query historical metrics of vertices.                                               | Read         | -                           | -             | coc:system:getTopologyVertexDetails           |
| coc::getTopologyEdgeDetails             | Provides the permission to query historical metrics of edges.                                                  | Read         | -                           | -             | coc:system:getTopologyEdgeDetails             |
| coc::listTopologyConfigurations         | Provides the permission to query topology configurations.                                                      | List         | -                           | -             | coc:system:listTopologyConfigurations         |
| coc::createTopologyConfigurations       | Provides the permission to create topology configurations.                                                     | Write        | -                           | -             | coc:system:createTopologyConfigurations       |
| coc::updateTopologyConfigurations       | Provides the permission to update topology configurations.                                                     | Write        | -                           | -             | coc:system:updateTopologyConfigurations       |
| coc::listCrossAccountEnterpriseProjects | Provides the permission to query the enterprise project list of a specified tenant in cross-account scenarios. | List         | -                           | -             | coc:system:listCrossAccountEnterpriseProjects |
| coc::getUserIdentity                    | Provides the permission to query the identity of a login user.                                                 | Read         | -                           | -             | coc:system:getUserIdentity                    |

| Action                            | Description                                                       | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------|-------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:template:list                 | Provides the permission to query the template list.               | List         | -                           | -             | -     |
| coc:template:get                  | Provides the permission to query template details.                | Read         | template*                   | -             | -     |
| coc:template:create               | Provides the permission to create a template.                     | Write        | -                           | -             | -     |
| coc:template:update               | Provides the permission to update a template.                     | Write        | template*                   | -             | -     |
| coc:template:delete               | Provides the permission to delete a template.                     | Write        | template*                   | -             | -     |
| coc:template:listVersions         | Provides the permission to query the template version list.       | List         | -                           | -             | -     |
| coc:template:getVersion           | Provides the permission to query the template version details.    | Read         | template*                   | -             | -     |
| coc:template:searchAuthorizations | Provides the permission to query the template authorization list. | List         | -                           | -             | -     |
| coc:template:createAuthorization  | Provides the permission to add template authorization.            | Write        | template*                   | -             | -     |

| Action                           | Description                                                     | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:template:deleteAuthorization | Provides the permission to delete template authorization.       | Write        | template *                  | -             | -     |
| coc:template:listConstraint      | Provides the permission to query the template constraint list.  | List         | -                           | -             | -     |
| coc:template:createConstraint    | Provides the permission to create a template constraint.        | Write        | template *                  | -             | -     |
| coc:template:updateConstraint    | Provides the permission to update a template constraint.        | Write        | template *                  | -             | -     |
| coc:template:deleteConstraint    | Provides the permission to delete a template constraint.        | Write        | template *                  | -             | -     |
| coc:templateInstance:create      | Provides the permission to create a template instance.          | Write        | -                           | -             | -     |
| coc:templateInstance:list        | Provides the permission to query the template instance list.    | List         | -                           | -             | -     |
| coc:templateInstance:get         | Provides the permission to query the template instance details. | Read         | template Instance *         | -             | -     |

| Action                             | Description                                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias                                  |
|------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|----------------------------------------|
| coc:templateInstance:listEvents    | Provides the permission to query the incident list of a template instance. | List         | template Instance *         | -             | -                                      |
| coc:templateInstance:listResources | Provides the permission to query the resource list of a template instance. | List         | template Instance *         | -             | -                                      |
| coc:templateInstance:delete        | Provides the permission to delete a template instance.                     | Write        | template Instance *         | -             | -                                      |
| coc:templateInstance:createRetry   | Provides the permission to retry template instance creation.               | Write        | -                           | -             | -                                      |
| coc::getBiBackboneNetworkTopo      | Provides the permission to query the BI backbone network topology.         | Read         | -                           | -             | coc:system:getBiBackboneNetworkTopo    |
| coc::updateBiBackboneNetworkTopo   | Provides the permission to modify the BI backbone network topology.        | Write        | -                           | -             | coc:system:updateBiBackboneNetworkTopo |
| coc::getBiBackboneNetworkTraffic   | Provides the permission to obtain backbone network traffic data.           | Read         | -                           | -             | coc:system:getBiBackboneNetworkTraffic |

| Action                                | Description                                                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias                                       |
|---------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------------|
| coc::refreshBiBackboneNetworkTopology | Provides the permission to refresh the backbone network topology.                         | Write        | -                           | -             | coc:system:refreshBiBackboneNetworkTopology |
| coc::getBiBackboneNetworkMetrics      | Provides the permission to obtain backbone network bandwidth data.                        | Read         | -                           | -             | coc:system:getBiBackboneNetworkMetrics      |
| coc::getBiScreenConfig                | Provides the permission to obtain BI dashboard configuration parameters.                  | Read         | -                           | -             | coc:system:getBiScreenConfig                |
| coc::updateBiScreenConfig             | Provides the permission to modify BI dashboard configurations.                            | Write        | -                           | -             | coc:system:updateBiScreenConfig             |
| coc::getBiResourceAlarmResourceInfos  | Provides the permission to obtain resource information from the resource alarm dashboard. | Read         | -                           | -             | coc:system:getBiResourceAlarmResourceInfos  |
| coc::getBiResourceAlarmAlarmInfos     | Provides the permission to obtain alarm information from the resource alarm dashboard.    | Read         | -                           | -             | coc:system:getBiResourceAlarmAlarmInfos     |
| coc::createAlarmFilterTemplate        | Provides the permission to create an original alarm filter template.                      | Write        | -                           | -             | coc:system:createAlarmFilterTemplate        |

| Action                            | Description                                                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias                                |
|-----------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------|
| coc::deleteAlarmFilterTemplate    | Provides the permission to delete an original alarm filter template.                       | Write        | -                           | -             | coc:system:deleteAlarmFilterTemplate |
| coc::listAlarmFilterTemplate      | Provides the permission to query the original alarm filter template list.                  | List         | -                           | -             | coc:system:listAlarmFilterTemplate   |
| coc::getResourceTopology          | Provides the permission to query resource topology details.                                | Read         | -                           | -             | coc:system:getResourceTopology       |
| coc::listConfigurationItem        | Provides the permission to view the configuration item list.                               | List         | -                           | -             | coc:system:listConfigurationItem     |
| coc:ciRelationshipBaseline:create | Provides the permission to create a new configuration item relationship baseline.          | Write        | -                           | -             | -                                    |
| coc:ciRelationshipBaseline:delete | Provides the permission to delete an existing configuration item relationship baseline.    | Write        | ciRelationshipBaseline*     | -             | -                                    |
| coc:ciRelationshipBaseline:get    | Provides the permission to view the details of a configuration item relationship baseline. | Read         | ciRelationshipBaseline*     | -             | -                                    |

| Action                            | Description                                                                             | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| coc:ciRelationshipBaseline:list   | Provides the permission to view the list of configuration item relationship baselines.  | List         | -                           | -             | -     |
| coc:ciRelationshipBaseline:update | Provides the permission to update an existing configuration item relationship baseline. | Write        | ciRelationshipBaseline*     | -             | -     |

Each API of COC usually supports one or more actions. [Table 3-291](#) lists the supported actions and dependencies.

**Table 3-291** Actions and dependencies supported by APIs

| API                          | Action                            | Related Action |
|------------------------------|-----------------------------------|----------------|
| GET /v1/resources/count      | coc:instance:countResources       | -              |
| GET /v1/applications         | coc:application:list              | -              |
| POST /v1/applications        | coc:application:create            | -              |
| PUT /v1/applications/{id}    | coc:application:update            | -              |
| DELETE /v1/applications/{id} | coc:application:delete            | -              |
| POST /v1/groups              | coc:application:createGroup       | -              |
| GET /v1/groups               | coc:application:listGroups        | -              |
| PUT /v1/groups/{id}          | coc:application:updateGroup       | -              |
| DELETE /v1/groups/{id}       | coc:application:deleteGroup       | -              |
| POST /v1/groups/{id}/sync    | coc:application:syncGroupResource | -              |

| API                                    | Action                                 | Related Action |
|----------------------------------------|----------------------------------------|----------------|
| PUT /v1/group-resource-relations       | coc:application:updateResources        | -              |
| POST /v1/group-resource-relations      | coc:application:addResources           | -              |
| DELETE /v1/group-resource-relations    | coc:application:removeResources        | -              |
| GET /v1/group-resource-relations       | coc:application:listResources          | -              |
| GET /v1/group-resource-relations/count | coc:application:countResourceRelations | -              |
| POST /v1/other-resources/import        | coc:instance:syncResources             | -              |
| POST /v1/components                    | coc:application:create                 | -              |
| GET /v1/components                     | coc:application:list                   | -              |
| PUT /v1/components/{id}                | coc:application:update                 | -              |
| DELETE /v1/components/{id}             | coc:application:delete                 | -              |
| GET /v1/application-view/search        | coc:application:list                   | -              |
| POST /v1/capacity                      | coc:application:getCapacity            | -              |
| GET /v1/capacity/order                 | coc:application:getSortedCapacity      | -              |
| POST /v1/vendor-account                | coc:vendorAccount:create               | -              |
| GET /v1/vendor-account                 | coc:vendorAccount:list                 | -              |
| PUT /v1/vendor-account                 | coc:vendorAccount:update               | -              |
| DELETE /v1/vendor-account              | coc:vendorAccount:delete               | -              |
| GET /v1/multicloud-resources/count     | coc:instance:countResources            | -              |
| POST /v1/multicloud-resources/sync     | coc:instance:syncResources             | -              |
| GET /v1/resource/views                 | coc:resourceView:list                  | -              |
| POST /v1/resource/views                | coc:resourceView:create                | -              |
| PUT /v1/resource/views/{id}            | coc:resourceView:update                | -              |
| DELETE /v1/resource/views/{id}         | coc:resourceView:delete                | -              |



| API                                           | Action                           | Related Action |
|-----------------------------------------------|----------------------------------|----------------|
| POST /v1/resource/views/{id}/sync             | coc:resourceView:syncResources   | -              |
| GET /v1/resource/views/resources              | coc:resourceView:listResources   | -              |
| GET /v1/resource/views/resources/count        | coc:resourceView:countResources  | -              |
| GET /v1/other-resources                       | coc:instance:listResources       | -              |
| DELETE /v1/other-resources                    | coc:instance:syncResources       | -              |
| PUT /v1/other-resources/{id}                  | coc:instance:syncResources       | -              |
| GET /v1/other-resources/count                 | coc:instance:countOtherResources | -              |
| GET /v1/resources/{resource_id}/tags          | coc:instance:listTagsForResource | -              |
| POST /v1/resources/{resource_id}/tags         | coc:instance:addResourceToTags   | -              |
| POST /v1/resources/uniagent/sync              | coc:instance:syncResources       | -              |
| POST /v1/other-resources/uniagent/sync        | coc:instance:syncResources       | -              |
| GET /v1/enterprise-project-collect            | coc::listEpsCollection           | -              |
| PUT /v1/enterprise-project-collect            | coc::updateEpsCollection         | -              |
| GET /v1/multicloud-resources/last-sync-status | coc::getLastSyncStatus           | -              |
| GET /v1/jobs/{job_id}                         | coc::getResourceSyncJob-Detail   | -              |
| GET /v1/multicloud-resources                  | coc:instance:listResources       | -              |
| GET /v1/application-model/next                | coc:application:listModel        | -              |
| POST /v1/application-view/batch-create        | coc:application:create           | -              |
| GET /v1/resources                             | coc:instance:listResources       | -              |
| GET /v1/resources/multi-count                 | coc:instance:countResources      | -              |

| API                                                  | Action                              | Related Action                                                                       |
|------------------------------------------------------|-------------------------------------|--------------------------------------------------------------------------------------|
| POST /v1/schedule/task                               | coc:schedule:create                 | iam:agencies:pass<br>(Provides the permission to pass an agency to a cloud service.) |
| GET /v1/schedule/task                                | coc:schedule:list                   | -                                                                                    |
| PUT /v1/schedule/task/{task_id}                      | coc:schedule:update                 | iam:agencies:pass<br>(Provides the permission to pass an agency to a cloud service.) |
| GET /v1/schedule/task/{task_id}                      | coc:schedule:get                    | -                                                                                    |
| DELETE /v1/schedule/task/{task_id}                   | coc:schedule:delete                 | -                                                                                    |
| POST /v1/schedule/task/{task_id}/enable              | coc:schedule:enable                 | -                                                                                    |
| POST /v1/schedule/task/{task_id}/disable             | coc:schedule:disable                | -                                                                                    |
| GET /v1/schedule/task/history                        | coc:schedule:getHistories           | -                                                                                    |
| POST /v1/alarm-mgmt/alarm/{alarm_id}/auto-process    | coc:instance:executeDocument        | -                                                                                    |
| POST /v1/alarm-mgmt/alarms/cancel                    | coc:alarm:clear                     | -                                                                                    |
| POST /v1/alarm-mgmt/alarms-linked-incident           | coc:alarm:createAlarmLinkedIncident | -                                                                                    |
| GET /v1/alarm-mgmt/alarm/{alarm_id}/handle-histories | coc:alarm:listHandleHistories       | -                                                                                    |
| GET /v1/alarm-mgmt/alarm/{alarm_id}                  | coc:alarm:get                       | -                                                                                    |
| POST /v2/incidents/{incident_id}/actions             | coc:ticket:action                   | -                                                                                    |
| POST /v2/incidents/list                              | coc:ticket:list                     | -                                                                                    |
| POST /v2/incidents/{incident_id}/histories           | coc:ticket:getOperationHistories    | -                                                                                    |
| GET /v2/incidents/{incident_id}/tasks                | coc:ticket:listActions              | -                                                                                    |

| API                                            | Action                           | Related Action |
|------------------------------------------------|----------------------------------|----------------|
| POST /v1/external/incident/create              | coc:ticket:create                | -              |
| POST /v1/external/incident/attachments         | coc:ticket:uploadFile            | -              |
| POST /v1/external/incident/handle              | coc:ticket:action                | -              |
| POST /v1/external/{ticket_type}/list-histories | coc:ticket:getOperationHistories | -              |
| POST /v1/external/list/authorizable-tickets    | coc:ticket:listAuthorizable      | -              |
| GET /v1/incident-tickets                       | coc:ticket:list                  | -              |
| GET /v1/external/incident/{incident_num}       | coc:ticket:get                   | -              |
| POST /v1/external/issues/create                | coc:ticket:create                | -              |
| GET /v1/external/issues/{ticket_id}            | coc:ticket:get                   | -              |
| POST /v1/external/warrooms                     | coc:warroom:create               | -              |
| POST /v1/external/warrooms/list                | coc:warroom:list                 | -              |
| POST /v1/instances/batches                     | coc:instance:autoBatchInstances  | -              |
| POST /v1/job/analyze-job                       | coc:document:analyzeRisk         | -              |
| POST /v1/job/scripts/{script_uuid}             | coc:instance:executeDocument     | -              |
| POST /v1/job/public-scripts/{script_uuid}      | coc:instance:executeDocument     | -              |
| GET /v1/job/scripts                            | coc:document:list                | -              |
| GET /v1/job/scripts/{script_uuid}              | coc:document:get                 | -              |
| POST /v1/job/scripts                           | coc:document:create              | -              |
| PUT /v1/job/scripts/{script_uuid}              | coc:document:update              | -              |
| DELETE /v1/job/scripts/{script_uuid}           | coc:document:delete              | -              |
| POST /v1/job/scripts/{script_uuid}/action      | coc:document:update              | -              |

| API                                                            | Action                                  | Related Action |
|----------------------------------------------------------------|-----------------------------------------|----------------|
| GET /v1/job/public-scripts                                     | coc:document:list                       | -              |
| GET /v1/job/public-scripts/{script_uuid}                       | coc:document:get                        | -              |
| GET /v1/job/script/orders                                      | coc:job:list                            | -              |
| GET /v1/job/script/orders/{execute_uuid}                       | coc:job:get                             | -              |
| GET /v1/job/script/orders/{execute_uuid}/batches/{batch_index} | coc:job:get                             | -              |
| GET /v1/job/script/orders/{execute_uuid}/batches               | coc:job:get                             | -              |
| GET /v1/job/script/orders/{execute_uuid}/statistics            | coc:job:get                             | -              |
| PUT /v1/job/script/orders/{execute_uuid}/operation             | coc:job:action                          | -              |
| GET /v1/documents                                              | coc:document:createDocument             | -              |
| POST /v1/documents                                             | coc:document:listDocument               | -              |
| GET /v1/atomics                                                | coc:documentAtomic:list                 | -              |
| GET /v1/atomics/{atomic_unique_key}                            | coc:documentAtomic:get                  | -              |
| PUT /v1/documents/{document_id}                                | coc:document:updateDocument             | -              |
| POST /v1/documents/{document_id}                               | coc:document:execute                    | -              |
| GET /v1/documents/{document_id}                                | coc:document:getDocument                | -              |
| DELETE /v1/documents/{document_id}                             | coc:document:deleteDocument             | -              |
| GET /v1/executions/{execution_id}                              | coc:execution:get                       | -              |
| GET /v1/executions/{execution_id}/steps                        | coc:execution:listExecutionStep         | -              |
| GET /v1/executions                                             | coc:execution:list                      | -              |
| GET /v1/executions/instances                                   | coc:execution:listExecutionStepInstance | -              |

| API                                                      | Action                    | Related Action |
|----------------------------------------------------------|---------------------------|----------------|
| POST /v1/executions                                      | coc:execution:operate     | -              |
| GET /v1/patch/instance/compliant                         | coc:complianceReport:list | -              |
| GET /v1/patch/instance/compliant/{instance_compliant_id} | coc:complianceReport:get  | -              |

## Resource Types (Resource)

A resource type indicates the resource to which a policy applies to. If you specify a resource type for any action in [Table 3-292](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in a policy to define resource types.

The following table lists the resource types that you can define in policy statements for COC.

**Table 3-292** Resource types supported by COC

| Resource Type   | URN                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| instance        | <ul style="list-style-type: none"> <li>ecs:&lt;region&gt;:&lt;account-id&gt;:instance:&lt;server-id&gt;</li> <li>bms:&lt;region&gt;:&lt;account-id&gt;:instance:&lt;server-id&gt;</li> <li>rds:&lt;region&gt;:&lt;account-id&gt;:instance:&lt;server-id&gt;</li> <li>gaussdb:&lt;region&gt;:&lt;account-id&gt;:instance:&lt;server-id&gt;</li> </ul> |
| document        | coc::<account-id>:document:<document-name>                                                                                                                                                                                                                                                                                                           |
| application     | coc::<account-id>:application:<application-code>                                                                                                                                                                                                                                                                                                     |
| resourceView    | coc::<account-id>:resourceView:<resourceViewId>                                                                                                                                                                                                                                                                                                      |
| schedule        | coc::<account-id>:schedule:<schedule-id>                                                                                                                                                                                                                                                                                                             |
| job             | coc::<account-id>:job:<job-id>                                                                                                                                                                                                                                                                                                                       |
| faultMode       | coc::<account-id>:faultMode:<fault-mode-id>                                                                                                                                                                                                                                                                                                          |
| contingencyPlan | coc::<account-id>:contingencyPlan:<contingency-plan-id>                                                                                                                                                                                                                                                                                              |
| attackTask      | coc::<account-id>:attackTask:<attack-task-name>                                                                                                                                                                                                                                                                                                      |
| attackRecord    | coc::<account-id>:attackRecord:<attack-record-id>                                                                                                                                                                                                                                                                                                    |
| drillTask       | coc::<account-id>:drillTask:<drill-task-id>                                                                                                                                                                                                                                                                                                          |

| Resource Type          | URN                                                             |
|------------------------|-----------------------------------------------------------------|
| attackTargetRecord     | coc::<account-id>:attackTargetRecord:<attack-target-record-id>  |
| drillRecord            | coc::<account-id>:drillRecord:<drill-record-id>                 |
| drillPlan              | coc::<account-id>:drillPlan:<drill-plan-id>                     |
| slaTemplate            | coc::<account-id>:slaTemplate:<sla_template-id>                 |
| parameter              | coc:<region>:<account-id>:parameter:<parameter-name>            |
| accountBaseline        | coc::<account-id>:accountBaseline:<account_baseline-id>         |
| provisionedProduct     | coc::<account-id>:provisionedProduct:<provisioned-product-id>   |
| product                | coc::<account-id>:product:<product-id>                          |
| portfolio              | coc::<account-id>:portfolio:<portfolio-id>                      |
| sloDiagram             | coc::<account-id>:sloDiagram:<diagram-id>                       |
| template               | coc::<account-id>:template:<template-id>                        |
| templateInstance       | coc::<account-id>:templateInstance:<template-instance-id>       |
| vm                     | coc::<account-id>:vm:<supplier>/<resource-id>                   |
| ciRelationshipBaseline | coc::<account-id>:ciRelationshipBaseline:<template-instance-id> |

## Conditions

A condition element lets you specify conditions for when an identity policy is in effect. It contains **condition keys** and **operators**.

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **bms:**) only apply to operations of the COC service. For details, see [Table 3-293](#).
  - The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a

request can originate from at most one VPC endpoint, so g:SourceVpce is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so g:TagKeys is a multivalued condition key.

- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For details about supported operators, see [Condition operators](#).

The following table lists the condition keys that you can define in identity policies for COC. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-293** Service-specific condition keys supported by COC

| Service-specific condition key | Type    | Single-valued/<br>Multivalued | Description                                                                            |
|--------------------------------|---------|-------------------------------|----------------------------------------------------------------------------------------|
| coc:TicketLevel                | String  | Single-valued                 | Filters access based on the ticket level in the request parameter.                     |
| coc:TicketCurrentHandlers      | String  | Multivalued                   | Filters access based on the ticket operator in the request parameter.                  |
| coc:TicketStatus               | String  | Single-valued                 | Filters access based on the ticket status in the request parameter.                    |
| coc:TicketType                 | String  | Single-valued                 | Filters access based on the ticket type in the request parameter.                      |
| coc:TicketBeginTime            | date    | Single-valued                 | Filters access based on the ticket start time in the request parameter.                |
| coc:TicketEndTime              | date    | Single-valued                 | Filters access based on the ticket end time in the request parameter.                  |
| coc:OperatorName               | String  | Single-valued                 | Filters access based on the operator in the request parameter.                         |
| coc:RequestTarget              | String  | Single-valued                 | Filters access based on the privilege escalation application in the request parameter. |
| coc:TicketTarget               | String  | Multivalued                   | Filters access based on the ticket application in the request parameter.               |
| coc:TicketScope                | String  | Multivalued                   | Filters access based on the ticket scope in the request parameter.                     |
| coc:RequestScope               | String  | Single-valued                 | Filters access based on the privilege escalation scope in the request.                 |
| coc:EscapeSwitchsEnabled       | boolean | Single valued                 | Filters access based on the escape feature in the request parameter.                   |

| Service-specific condition key | Type   | Single-valued/Multivalued | Description                                                                                |
|--------------------------------|--------|---------------------------|--------------------------------------------------------------------------------------------|
| coc:Creator                    | String | Single-valued             | Filters access based on the creator of resource in COC.                                    |
| coc:Executor                   | String | Single-valued             | Filters access based on the executor specified by the service ticket in COC.               |
| coc:DocumentRiskLevel          | String | Single-valued             | Filters access based on the document risk level specified in the request parameter.        |
| coc:JobType                    | String | Single-valued             | Filters access based on the service ticket type specified in the request parameter.        |
| coc:Application Code           | String | Multivalued               | Filters access based on the application code specified in the request parameter.           |
| coc:Application GroupCode      | String | Single-valued             | Filters access based on the application group code specified in the request parameter.     |
| coc:AttackTargetType           | String | Single-valued             | Filters access based on the attack target type specified in the request parameter.         |
| coc:QuickSetup Type            | String | Single-valued             | Filters access based on the request configuration type specified in the request parameter. |

### 3.14.17 Application Performance Management (APM)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)



This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by APM, see [Resources](#).

- **Condition Key** contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by APM, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for APM.

**Table 3-294** Supported actions

| Action                         | Description                                                             | Access Level          | Resource Type (*: required) | Condition Key                | Alias                           |
|--------------------------------|-------------------------------------------------------------------------|-----------------------|-----------------------------|------------------------------|---------------------------------|
| apm:application:list           | Grants permission to obtain the information about the application list. | List                  | -                           | -                            | apm:apm2BusinessBusiness:list   |
| apm:application:getService     | Grants permission to obtain service information.                        | Read                  | -                           | <b>g:EnterpriseProjectId</b> | apm:apm2Service:get             |
| apm::retrieveCredential        | Grants permission to obtain an access credential.                       | Permission_management | -                           | -                            | apm:apm2ApiKey:read             |
| apm::createCredential          | Grants permission to create an access credential.                       | Permission_management | -                           | -                            | apm:apm2ApiKey:create           |
| apm::deleteCredential          | Grants permission to delete an access credential.                       | Permission_management | -                           | -                            | apm:apm2ApiKey:delete           |
| apm:application:get            | Grants permission to obtain the information about an application.       | Read                  | -                           | <b>g:EnterpriseProjectId</b> | apm:apm2BusinessBusiness:get    |
| apm:application:updateInstance | Grants permission to modify an instance.                                | Write                 | -                           | <b>g:EnterpriseProjectId</b> | apm:apm2BusinessInstance:update |

| Action                                | Description                                                 | Access Level | Resource Type (*: required) | Condition Key                         | Alias                                                     |
|---------------------------------------|-------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-----------------------------------------------------------|
| apm:application:deleteInstance        | Grants permission to delete an instance.                    | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | apm:apm2BusinessInstance:delete                           |
| apm:application:getInstance           | Grants permission to obtain instance data.                  | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | apm:apm2BusinessInstance:get                              |
| apm:application:getEnv                | Grants permission to obtain environment information.        | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | apm:apm2BusinessEnv:get                                   |
| apm:application:getMonitorItemConf    | Grants permission to obtain monitoring item configurations. | Read         | -                           | <a href="#">g:EnterpriseProjectId</a> | apm:apm2BusinessMonitorItem:get                           |
| apm:application:updateMonitorItemConf | Grants permission to modify monitoring item configurations. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | apm:apm2BusinessMonitorItem:update                        |
| apm:application:delete                | Grants permission to delete an application.                 | Write        | -                           | <a href="#">g:EnterpriseProjectId</a> | apm:apm2BusinessBusiness:delete                           |
| apm::getTopology                      | Grants permission to obtain topology data.                  | Read         | -                           | -                                     | apm:apm2BusinessTopology:get<br>apm:apm2TraceTopology:get |

| Action                              | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                                                                               |
|-------------------------------------|-----------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|-------------------------------------------------------------------------------------|
| apm::updateConf                     | Grants permission to modify configurations.                     | Write        | -                           | -                                             | apm:apm2Service:update                                                              |
| apm:application:getTransaction      | Grants permission to obtain transaction data.                   | Read         | -                           | <a href="#">g:EnterpriseProjectId</a>         | apm:apm2BusinessBusiness:get                                                        |
| apm::createAdminInfo                | Grants permission to create system management information.      | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>         | apm:apm2Admin:create                                                                |
| apm:application:update              | Grants permission to modify an application.                     | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>         | apm:apm2BusinessBusiness:update                                                     |
| apm::getConf                        | Grants permission to obtain configurations.                     | Read         | -                           | -                                             | apm:apm2BusinessView:get<br>apm:apm2Service:get                                     |
| apm:application:getTraceEvents      | Grants permission to obtain the data of self-developed tracing. | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>         | apm:apm2TraceEvent:get<br>apm:apm2TraceEvents:get<br>apm:apm2BusinessSpanSearch:get |
| apm:application:listTagsForResource | Grants permission to query the application tag list.            | Read         | application*                | -                                             | apm:apm2BusinessBusiness:list                                                       |
|                                     |                                                                 |              | -                           | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                                                                     |

| Action                        | Description                                                | Access Level | Resource Type (*: required) | Condition Key                                 | Alias                            |
|-------------------------------|------------------------------------------------------------|--------------|-----------------------------|-----------------------------------------------|----------------------------------|
| apm:application:tagResource   | Grants permission to create application tags.              | Tagging      | application *               | -                                             | apm:apm2BusinessBusiness: list   |
|                               |                                                            |              | -                           | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                  |
| apm:application:unTagResource | Grants permission to delete application tags.              | Tagging      | application *               | -                                             | apm:apm2BusinessBusiness: list   |
|                               |                                                            |              | -                           | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a> |                                  |
| apm:application:create        | Grants permission to create an application.                | Write        | -                           | <a href="#">g:EnterpriseProjectId</a>         | apm:apm2BusinessBusiness: create |
| apm::deleteAdminInfo          | Grants permission to delete system management information. | Write        | -                           | -                                             | apm:apm2Admin:delete             |
| apm::getAdminInfo             | Grants permission to query system management information.  | Read         | -                           | -                                             | apm:apm2Admin:get                |
| apm::updateAdminInfo          | Grants permission to update system management information. | Write        | -                           | -                                             | apm:apm2Admin:update             |
| apm::getAlarmData             | Grants permission to obtain alarm data.                    | Read         | -                           | -                                             | apm:apm2BusinessBusiness: get    |
| apm::createAlarmRule          | Grants permission to create an alarm rule.                 | Write        | -                           | -                                             | apm:apm2BusinessBusiness: create |

| Action                | Description                                       | Access Level          | Resource Type (*: required) | Condition Key | Alias                           |
|-----------------------|---------------------------------------------------|-----------------------|-----------------------------|---------------|---------------------------------|
| apm::deleteAlarmRule  | Grants permission to delete an alarm rule.        | Write                 | -                           | -             | apm:apm2BusinessBusiness:delete |
| apm::getAlarmRule     | Grants permission to query an alarm rule.         | Read                  | -                           | -             | apm:apm2BusinessBusiness:get    |
| apm::listAlarmRule    | Grants permission to query the alarm rule list.   | List                  | -                           | -             | apm:apm2BusinessBusiness:get    |
| apm::updateAlarmRule  | Grants permission to modify an alarm rule.        | Write                 | -                           | -             | apm:apm2BusinessBusiness:update |
| apm::updateCredential | Grants permission to modify an access credential. | Permission management | -                           | -             | apm:apm2AccessKeys:update       |

Each API of APM usually supports one or more actions. [Table 3-295](#) lists the supported actions and dependencies.

**Table 3-295** Actions and dependencies supported by APM APIs

| API                              | Action                  | Dependency |
|----------------------------------|-------------------------|------------|
| GET /v1/apm2/access-keys         | apm::retrieveCredential | -          |
| POST /v1/apm2/access-keys        | apm::createCredential   | -          |
| DELETE /v1/apm2/access-keys/{ak} | apm::deleteCredential   | -          |

| API                                                                          | Action                                | Dependency |
|------------------------------------------------------------------------------|---------------------------------------|------------|
| POST /v1/apm2/openapi/alarm/data/get-alarm-data-list                         | apm:application:get                   | -          |
| POST /v1/apm2/openapi/alarm/data/get-alarm-notify-list                       | apm:application:get                   | -          |
| POST /v1/apm2/openapi/apm-service/agent-mgr/change-status                    | apm:application:updateInstance        | -          |
| POST /v1/apm2/openapi/apm-service/agent-mgr/delete-agent                     | apm:application:deleteInstance        | -          |
| POST /v1/apm2/openapi/apm-service/agent-mgr/search                           | apm:application:getInstance           | -          |
| POST /v1/apm2/openapi/apm-service/app-mgr/search                             | apm:application:getEnv                | -          |
| POST /v1/apm2/openapi/apm-service/monitor-item-mgr/get-env-monitor-item-list | apm:application:getMonitorItemConf    | -          |
| GET /v1/apm2/openapi/apm-service/monitor-item-mgr/get-monitor-item-detail    | apm:application:getMonitorItemConf    | -          |
| POST /v1/apm2/openapi/apm-service/monitor-item-mgr/save-monitor-item-config  | apm:application:updateMonitorItemConf | -          |
| DELETE /v1/apm2/openapi/cmdb/apps/delete-app/{application_id}                | apm:application:delete                | -          |

| API                                                                                              | Action                     | Dependency |
|--------------------------------------------------------------------------------------------------|----------------------------|------------|
| GET /v1/apm2/<br>openapi/cmdb/<br>apps/get-apps                                                  | apm:application:get        | -          |
| GET /v1/apm2/<br>openapi/cmdb/<br>business/get-<br>business-detail/<br>{business_id}             | apm:application:get        | -          |
| GET /v1/apm2/<br>openapi/cmdb/<br>business/get-<br>business-list                                 | apm:application:list       | -          |
| GET /v1/apm2/<br>openapi/cmdb/<br>envs/get-app-envs                                              | apm:application:getEnv     | -          |
| GET /v1/apm2/<br>openapi/cmdb/sub-<br>business/get-sub-<br>business-detail/<br>{sub_business_id} | apm:application:get        | -          |
| POST /v1/apm2/<br>openapi/cmdb/tag/<br>get-env-tag-list                                          | apm:application:get        | -          |
| GET /v1/apm2/<br>openapi/cmdb/<br>topology-trees/get-<br>topology-trees                          | apm::getTopology           | -          |
| GET /v1/apm2/<br>openapi/region/get-<br>all-supported-<br>region                                 | apm:application:getService | -          |
| GET /v1/apm2/<br>openapi/region/get-<br>opened-region                                            | apm:application:getService | -          |
| GET /v1/apm2/<br>openapi/<br>systemmng/get-ak-<br>sk-list                                        | apm::retrieveCredential    | -          |
| GET /v1/apm2/<br>openapi/<br>systemmng/get-<br>master-address                                    | apm:application:getService | -          |



| API                                                                 | Action                         | Dependency |
|---------------------------------------------------------------------|--------------------------------|------------|
| POST /v1/apm2/openapi/topology/business-search                      | apm:application:getTransaction | -          |
| POST /v1/apm2/openapi/topology/env-search                           | apm:application:getTransaction | -          |
| POST /v1/apm2/openapi/tracing/access/get-access-point/{business_id} | apm:application:get            | -          |
| POST /v1/apm2/openapi/tracing/business/create                       | apm::createAdminInfo           | -          |
| GET /v1/apm2/openapi/tracing/business/token/{business_id}           | apm:application:update         | -          |
| POST /v1/apm2/openapi/transaction/business-env                      | apm:application:get            | -          |
| POST /v1/apm2/openapi/transaction/detail                            | apm:application:getTransaction | -          |
| POST /v1/apm2/openapi/transaction/search                            | apm:application:getTransaction | -          |
| POST /v1/apm2/openapi/transaction/transaction-config-search         | apm:application:getTransaction | -          |
| GET /v1/apm2/openapi/view/config/get-monitor-item-view-config       | apm::getConf                   | -          |
| POST /v1/apm2/openapi/view/mainview/get-env-instance-list           | apm:application:getInstance    | -          |

| API                                                          | Action                             | Dependency |
|--------------------------------------------------------------|------------------------------------|------------|
| GET /v1/apm2/openapi/view/mainview/get-env-monitor-item-list | apm:application:getMonitorItemConf | -          |
| POST /v1/apm2/openapi/view/metric/get-clob-detail            | apm::getConf                       | -          |
| POST /v1/apm2/openapi/view/metric/raw-table                  | apm::getConf                       | -          |
| POST /v1/apm2/openapi/view/metric/sum-table                  | apm::getConf                       | -          |
| POST /v1/apm2/openapi/view/metric/trend                      | apm::getConf                       | -          |
| POST /v1/apm2/openapi/view/profiling/flame-line-tree         | apm::getTopology                   | -          |
| GET /v1/apm2/openapi/view/trace/get-event-detail             | apm:application:getTraceEvents     | -          |
| GET /v1/apm2/openapi/view/trace/get-trace-events             | apm:application:getTraceEvents     | -          |
| POST /v1/apm2/openapi/view/trace/span-search                 | apm:application:getTraceEvents     | -          |
| GET /v1/apm2/openapi/view/trace/topology                     | apm::getTopology                   | -          |
| POST /v2/alarm/data/get-alarm-data-list                      | apm:application:get                | -          |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-296](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource

element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for APM.

**Table 3-296** Resource types supported by APM

| Resource Type | URN                                            |
|---------------|------------------------------------------------|
| application   | apm::<account-id>:application:<application-id> |

## Conditions

APM does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.14.18 Application Operations Management

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The Access Level column describes how the action is classified (List, Read, or Write). This classification helps you understand the level of access that an action grants when you use it in an identity policy.

- The Resource Type column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by AOM, see [Resources](#).

- The Condition Key column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the Resource Type column has values for an action, the condition key takes effect only for the listed resource types.
  - If the Resource Type column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the Condition Key column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by AOM, see [Conditions](#).

- The Alias column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for AOM.

**Table 3-297** Actions supported by AOM

| Action            | Description                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| aom:view:delete   | Grants permission to delete dashboard.                | Write        | -                           | -             | -     |
| aom:view:get      | Grants permission to get dashboard.                   | Read         | -                           | -             | -     |
| aom:metric:delete | Grants permission to delete monitoring configuration. | Write        | -                           | -             | -     |

| Action                    | Description                                                   | Access Level | Resource Type (*: required) | Condition Key | Alias          |
|---------------------------|---------------------------------------------------------------|--------------|-----------------------------|---------------|----------------|
| aom:icmgr:get             | Grants permission to get collection component version info.   | Read         | -                           | -             | -              |
| aom:agency:get            | Grants permission to querying agency permissions.             | Read         | -                           | -             | -              |
| aom:icmgr:list            | Grants permission to query ICAgent list.                      | List         | -                           | -             | -              |
| aom:metric:set            | Grants permission to modify monitoring configuration.         | Write        | -                           | -             | -              |
| aom:metric:list           | Grants permission to query metric item.                       | List         | -                           | -             | aom:metric:get |
| aom:metric:put            | Grants permission to report metric.                           | Write        | -                           | -             | -              |
| aom:discovery Rule:set    | Grants permission to create or update service discovery rule. | Write        | -                           | -             | -              |
| aom:discovery Rule:delete | Grants permission to delete service discovery rule.           | Write        | -                           | -             | -              |
| aom:discovery Rule:list   | Grants permission to list service discovery rule.             | List         | -                           | -             | -              |

| Action                     | Description                                      | Access Level | Resource Type (*: required) | Condition Key                                                                                                                         | Alias                   |
|----------------------------|--------------------------------------------------|--------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| aom:alarmRule:create       | Grants permission to create alarm rule.          | Write        | alarm Rule *                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -                       |
|                            |                                                  |              | -                           | <ul style="list-style-type: none"> <li>• <a href="#">g:TagKeys</a></li> <li>• <a href="#">g:RequestTag/&lt;tag-key&gt;</a></li> </ul> |                         |
| aom:alarmRule:list         | Grants permission to query alarm rule list.      | List         | -                           | -                                                                                                                                     | -                       |
| aom:alarmRule:update       | Grants permission to update alarm rule.          | Write        | -                           | -                                                                                                                                     | aom:alarmRule:set       |
| aom:alarmRule:delete       | Grants permission to delete alarm rule.          | Write        | alarm Rule *                | <a href="#">g:ResourceTag/&lt;tag-key&gt;</a>                                                                                         | -                       |
| aom:alarm:put              | Grants permission to push alarms and events.     | Write        | -                           | -                                                                                                                                     | -                       |
| aom:alarmRule:get          | Grants permission to query alarm rule.           | Read         | -                           | -                                                                                                                                     | -                       |
| aom:event2AlarmRule:list   | Grants permission to list event to alarm rule.   | List         | -                           | -                                                                                                                                     | -                       |
| aom:event2AlarmRule:create | Grants permission to create event to alarm rule. | Write        | -                           | -                                                                                                                                     | -                       |
| aom:event2AlarmRule:update | Grants permission to update event to alarm rule. | Write        | -                           | -                                                                                                                                     | aom:event2AlarmRule:set |

| Action                     | Description                                      | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------|--------------------------------------------------|--------------|-----------------------------|---------------|-------|
| aom:event2AlarmRule:delete | Grants permission to delete event to alarm rule. | Write        | -                           | -             | -     |
| aom:muteRule:create        | Grants permission to create mute rule.           | Write        | -                           | -             | -     |
| aom:muteRule:list          | Grants permission to list mute rule.             | List         | -                           | -             | -     |
| aom:muteRule:update        | Grants permission to update mute rule.           | Write        | -                           | -             | -     |
| aom:muteRule:delete        | Grants permission to delete mute rule.           | Write        | -                           | -             | -     |
| aom:actionRule:get         | Grants permission to query action rule.          | Read         | -                           | -             | -     |
| aom:actionRule:list        | Grants permission to query action rule list.     | List         | -                           | -             | -     |
| aom:actionRule:create      | Grants permission to create action rule.         | Write        | -                           | -             | -     |
| aom:actionRule:update      | Grants permission to update action rule.         | Write        | -                           | -             | -     |
| aom:actionRule:delete      | Grants permission to delete action rule.         | Write        | -                           | -             | -     |

| Action                          | Description                                           | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------|-------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| aom:alarm:list                  | Grants permission to query alarms and events.         | List         | -                           | -             | -     |
| aom:notificationTemplate:create | Grants permission to create notification template.    | Write        | -                           | -             | -     |
| aom:notificationTemplate:delete | Grants permission to delete notification template.    | Write        | -                           | -             | -     |
| aom:notificationTemplate:update | Grants permission to update notification template.    | Write        | -                           | -             | -     |
| aom:notificationTemplate:list   | Grants permission to get notification template list.  | List         | -                           | -             | -     |
| aom:notificationTemplate:get    | Grants permission to get notification template.       | Read         | -                           | -             | -     |
| aom:alarmRuleTemplate:list      | Grants permission to query alarm rule policy V4 list. | List         | -                           | -             | -     |
| aom:alarmRuleTemplate:delete    | Grants permission to delete alarm rule policy V4.     | Write        | -                           | -             | -     |



Each API of AOM usually supports one or more actions. [Table 3-298](#) lists the supported actions and dependencies.

**Table 3-298** Actions and dependencies supported by AOM APIs

| API                                                          | Action            | Dependencies |
|--------------------------------------------------------------|-------------------|--------------|
| DELETE /v2/{project_id}/aom/dashboards/{dashboard_id}        | aom:view:delete   | -            |
| GET /v2/{project_id}/aom/dashboards                          | aom:view:get      | -            |
| GET /v2/{project_id}/aom/dashboards/{dashboard_id}           | aom:view:get      | -            |
| DELETE /v2/{project_id}/aom/dashboards-folder/{folder_id}    | aom:view:delete   | -            |
| GET /v2/{project_id}/aom/dashboards-folder                   | aom:view:get      | -            |
| DELETE /v1/{project_id}/aom/prometheus                       | aom:metric:delete | -            |
| GET /v1/{project_id}/aom/prometheus                          | aom:metric:list   | -            |
| POST /v1/{project_id}/aom/prometheus                         | aom:metric:put    | -            |
| PUT /v1/{project_id}/aom/prometheus                          | aom:metric:set    | -            |
| POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/rules | aom:metric:put    | -            |
| GET /v1/{project_id}/access-code                             | aom:icmgr:get     | -            |

| API                                                       | Action          | Dependencies |
|-----------------------------------------------------------|-----------------|--------------|
| GET /v1/{project_id}/aom/auth/grant                       | aom:agency:get  | -            |
| GET /v1/{project_id}/{cluster_id}/{namespace}/agents      | aom:icmgr:list  | -            |
| POST /v2/{project_id}/series                              | aom:metric:list | -            |
| POST /v2/{project_id}/samples                             | aom:metric:list | -            |
| GET /v1/{project_id}/aom/api/v1/query_range               | aom:metric:list | -            |
| POST /v1/{project_id}/aom/api/v1/query_range              | aom:metric:list | -            |
| GET /v1/{project_id}/aom/api/v1/query                     | aom:metric:list | -            |
| POST /v1/{project_id}/aom/api/v1/query                    | aom:metric:list | -            |
| GET /v1/{project_id}/aom/api/v1/label/{label_name}/values | aom:metric:list | -            |
| GET /v1/{project_id}/aom/api/v1/labels                    | aom:metric:list | -            |
| POST /v1/{project_id}/aom/api/v1/labels                   | aom:metric:list | -            |
| GET /v1/{project_id}/aom/api/v1/metadata                  | aom:metric:list | -            |
| POST /v1/{project_id}/ams/metrics                         | aom:metric:list | -            |

| API                                                             | Action                   | Dependencies |
|-----------------------------------------------------------------|--------------------------|--------------|
| POST /v1/<br>{project_id}/ams/<br>metricdata                    | aom:metric:list          | -            |
| POST /v1/<br>{project_id}/ams/<br>report/metricdata             | aom:metric:put           | -            |
| PUT /v1/<br>{project_id}/inv/<br>servicediscoveryr-<br>ules     | aom:discoveryRule:set    | -            |
| DELETE /v1/<br>{project_id}/inv/<br>servicediscoveryr-<br>ules  | aom:discoveryRule:delete | -            |
| GET /v1/<br>{project_id}/inv/<br>servicediscoveryr-<br>ules     | aom:discoveryRule:list   | -            |
| POST /v2/<br>{project_id}/alarm-<br>rules                       | aom:alarmRule:create     | -            |
| GET /v2/<br>{project_id}/alarm-<br>rules                        | aom:alarmRule:list       | -            |
| PUT /v2/<br>{project_id}/alarm-<br>rules                        | aom:alarmRule:update     | -            |
| DELETE /v2/<br>{project_id}/alarm-<br>rules/<br>{alarm_rule_id} | aom:alarmRule:delete     | -            |
| GET /v2/<br>{project_id}/alarm-<br>rules/<br>{alarm_rule_id}    | aom:alarmRule:get        | -            |
| POST /v2/<br>{project_id}/alarm-<br>rules/delete                | aom:alarmRule:delete     | -            |
| POST /v2/<br>{project_id}/events                                | aom:alarm:list           | -            |

| API                                                 | Action                     | Dependencies |
|-----------------------------------------------------|----------------------------|--------------|
| POST /v2/{project_id}/events/statistic              | aom:alarm:list             | -            |
| PUT /v2/{project_id}/push/events                    | aom:alarm:put              | -            |
| GET /v2/{project_id}/alarm-notified-histories       | aom:alarm:list             | -            |
| GET /v2/{project_id}/event2alarm-rule               | aom:event2AlarmRule:list   | -            |
| POST /v2/{project_id}/event2alarm-rule              | aom:event2AlarmRule:create | -            |
| PUT /v2/{project_id}/event2alarm-rule               | aom:event2AlarmRule:update | -            |
| DELETE /v2/{project_id}/event2alarm-rule            | aom:event2AlarmRule:delete | -            |
| POST /v2/{project_id}/alert/action-rules            | aom:actionRule:create      | -            |
| GET /v2/{project_id}/alert/action-rules             | aom:actionRule:list        | -            |
| PUT /v2/{project_id}/alert/action-rules             | aom:actionRule:update      | -            |
| DELETE /v2/{project_id}/alert/action-rules          | aom:actionRule:delete      | -            |
| GET /v2/{project_id}/alert/action-rules/{rule_name} | aom:actionRule:get         | -            |
| POST /v2/{project_id}/alert/mute-rules              | aom:muteRule:create        | -            |

| API                                                      | Action                                                                                                                                                       | Dependencies |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| DELETE /v2/{project_id}/alert/mute-rules                 | aom:muteRule:delete                                                                                                                                          | -            |
| PUT /v2/{project_id}/alert/mute-rules                    | aom:muteRule:update                                                                                                                                          | -            |
| GET /v2/{project_id}/alert/mute-rules                    | aom:muteRule:list                                                                                                                                            | -            |
| POST /v4/{project_id}/alarm-rules                        | aom:alarmRule:create                                                                                                                                         | -            |
| GET /v4/{project_id}/alarm-rules                         | aom:alarmRule:list                                                                                                                                           | -            |
| DELETE /v4/{project_id}/alarm-rules                      | aom:alarmRule:delete<br><b>NOTE</b><br>The resource type <b>alarmRule</b> of this action applies only to the <b>DELETE /v4/{project_id}/alarm-rules</b> API. | -            |
| POST /v2/{project_id}/events/notification/templates      | aom:notificationTemplate:create                                                                                                                              | -            |
| DELETE /v2/{project_id}/events/notification/templates    | aom:notificationTemplate:delete                                                                                                                              | -            |
| PUT /v2/{project_id}/events/notification/templates       | aom:notificationTemplate:update                                                                                                                              | -            |
| GET /v2/{project_id}/events/notification/templates       | aom:notificationTemplate:list                                                                                                                                | -            |
| GET /v2/{project_id}/events/notification/template/{name} | aom:notificationTemplate:get                                                                                                                                 | -            |

| API                                          | Action                       | Dependencies |
|----------------------------------------------|------------------------------|--------------|
| DELETE /v4/{project_id}/alarm-rules-template | aom:alarmRuleTemplate:delete | -            |
| GET /v4/{project_id}/alarm-rules-template    | aom:alarmRuleTemplate:list   | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-299](#), the resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to resources of this type. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in an identity policy to define resource types.

The following table lists the resource types that you can define in identity policy statements for AOM.

**Table 3-299** Resource types supported by AOM

| Resource Type | URN                                                 |
|---------------|-----------------------------------------------------|
| alarmRule     | aom:<region>:<account-id>:alarmRule:<alarm_rule_id> |

## Conditions

AOM does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.14.19 Optimization Advisor

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [service control policies \(SCPs\)](#) for access control.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences Between IAM Policies and Organizations SCPs?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP policy, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (such as **list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by OA, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by OA, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for OA.

**Table 3-300** Actions supported by OA

| Action                       | Description                                              | Access Level | Resource Type (*: Required) | Condition Key | Alias                    |
|------------------------------|----------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------|
| oa::listAuthorizations       | Grants permission to obtain the user authorization list. | read         | -                           | -             | oa:authorizations:list   |
| oa::updateAuthorizations     | Grants permission to modify user authorizations.         | write        | -                           | -             | oa:authorizations:update |
| oa::deleteAuthorizations     | Grants permission to delete user authorizations.         | write        | -                           | -             | oa:authorizations:delete |
| oa:monthReports:list         | Grants permission to obtain the monthly report list.     | read         | -                           | -             | -                        |
| oa:monthReports:get          | Grants permission to get details about a monthly report. | read         | -                           | -             | -                        |
| oa:monthReports:download     | Grants permission to download a monthly report.          | read         | -                           | -             | -                        |
| oa:checkItemRules:update     | Grants permission to modify check item rules.            | write        | -                           | -             | -                        |
| oa:checkItemRules:list       | Grants permission to obtain check item rules.            | read         | -                           | -             | -                        |
| oa:autoCheckRule:update      | Grants permission to modify auto check rules.            | write        | -                           | -             | -                        |
| oa:autoCheckRule:get         | Grants permission to get auto check rules.               | read         | -                           | -             | -                        |
| oa:riskItemsCheck:createTask | Grants permission to create a risk check task.           | write        | -                           | -             | -                        |



| Action                                         | Description                                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|------------------------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| oa:riskItemsCheck:getTaskProgress              | Grants permission to obtain the progress of a risk check task.             | read         | -                           | -             | -     |
| oa:riskItemsCheck:getTaskResult                | Grants permission to obtain the risk check results.                        | read         | -                           | -             | -     |
| oa:riskItemsCheck:getTaskResultDimension       | Grants permission to obtain the dimensions of risk check results.          | read         | -                           | -             | -     |
| oa:riskItemsCheck:listReportSubscriptions      | Grants permission to obtain subscriptions to risk check reports.           | read         | -                           | -             | -     |
| oa:riskItemsCheck:getReportSubscriptionRule    | Grants permission to obtain the subscription rules for risk check reports. | read         | -                           | -             | -     |
| oa:riskItemsCheck:updateReportSubscriptionRule | Grants permission to modify the subscription rules for risk check reports. | write        | -                           | -             | -     |
| oa:riskItemsCheck:getRiskItemNum               | Grants permission to obtain the number of risky items.                     | read         | -                           | -             | -     |
| oa:riskItemsCheck:exportCheckItemResult        | Grants permission to export a risk check report.                           | read         | -                           | -             | -     |
| oa:riskItemsCheck:getExportProgress            | Grants permission to obtain the progress of exporting a risk check report. | read         | -                           | -             | -     |

| Action                                    | Description                                                                        | Access Level | Resource Type (*: Required) | Condition Key | Alias                           |
|-------------------------------------------|------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------|
| oa:riskItemsCheck:downloadCheckItemResult | Grants permission to download a risk check report.                                 | read         | -                           | -             | -                               |
| oa:riskItemCheck:createTask               | Grants permission to create a single-item risk check task.                         | write        | -                           | -             | -                               |
| oa:riskItemCheck:getTaskProgress          | Grants permission to obtain the progress of a single-item risk check task.         | read         | -                           | -             | -                               |
| oa:riskItemCheck:getTaskResult            | Grants permission to obtain the check results of a single risky item.              | read         | -                           | -             | -                               |
| oa:riskItemCheck:listTaskResultRegions    | Grants permission to obtain the list of sites for a single-item risk check report. | read         | -                           | -             | -                               |
| oa:riskItemsCheck:listCheckItems          | Grants permission to obtain the list of check item rules.                          | read         | -                           | -             | -                               |
| oa::saveWellArchitectedRecord             | Grants permission to save the well-architected questionnaire.                      | write        | -                           | -             | oa:wellArchitected:saveRecord   |
| oa::deleteWellArchitectedRecord           | Grants permission to delete the well-architected questionnaire.                    | write        | -                           | -             | oa:wellArchitected:deleteRecord |
| oa::listWellArchitectedRecord             | Grants permission to view the well-architected questionnaire list.                 | read         | -                           | -             | oa:wellArchitected:listRecord   |

| Action                                | Description                                                                                              | Access Level | Resource Type (*: Required) | Condition Key | Alias                              |
|---------------------------------------|----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|------------------------------------|
| oa::getWellArchitectedRecordDetail    | Grants permission to obtain well-architected questionnaire details.                                      | read         | -                           | -             | oa:wellArchitected:getRecordDetail |
| oa::generateWellArchitectedReport     | Grants permission to generate a well-architected report.                                                 | write        | -                           | -             | oa:wellArchitected:generateReport  |
| oa::getWellArchitectedReportDetail    | Grants permission to view well-architected report details.                                               | read         | -                           | -             | oa:wellArchitected:getReportDetail |
| oa::listOrgAccounts                   | Grants permission to obtain the list of organization member accounts.                                    | read         | -                           | -             | oa:riskItemsCheck:listOrgAccounts  |
| oa:capacityAnalysis:getConfig         | Grants permission to obtain capacity optimization analysis settings.                                     | read         | -                           | -             | -                                  |
| oa:capacityAnalysis:updateConfig      | Grants permission to modify capacity optimization analysis settings.                                     | write        | -                           | -             | -                                  |
| oa:capacityAnalysis:listResourceTypes | Grants permission to obtain the resource types for applying the capacity optimization analysis settings. | read         | -                           | -             | -                                  |
| oa:capacityAnalysis:listResources     | Grants permission to obtain the resources for applying the capacity optimization analysis settings.      | read         | -                           | -             | -                                  |

| Action                                  | Description                                                                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| oa:capacityAnalysis:listResourceGroups  | Grants permission to obtain the resource groups for applying the capacity optimization analysis settings. | read         | -                           | -             | -     |
| oa:capacityAnalysis:createJob           | Grants permission to create a capacity optimization analysis task.                                        | write        | -                           | -             | -     |
| oa:capacityAnalysis:getJobProgress      | Grants permission to obtain the progress of a capacity optimization analysis task.                        | read         | -                           | -             | -     |
| oa:capacityAnalysis:stopJob             | Grants permission to stop a capacity optimization analysis task.                                          | write        | -                           | -             | -     |
| oa:capacityAnalysis:getResultSummary    | Grants permission to obtain the summary of capacity optimization analysis results.                        | read         | -                           | -             | -     |
| oa:capacityAnalysis:listResultDetails   | Grants permission to obtain the details of capacity optimization analysis results.                        | read         | -                           | -             | -     |
| oa:capacityAnalysis:deleteResultDetails | Grants permission to delete the details of capacity optimization analysis results.                        | write        | -                           | -             | -     |

| Action                                       | Description                                                                                     | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------------------|-------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| oa:capacityAnalysis:listReports              | Grants permission to obtain the list of capacity optimization analysis reports.                 | read         | -                           | -             | -     |
| oa:capacityAnalysis:deleteReport             | Grants permission to delete a capacity optimization analysis report.                            | write        | -                           | -             | -     |
| oa:capacityAnalysis:getReportExport-Progress | Grants permission to obtain the progress for exporting a capacity optimization analysis report. | read         | -                           | -             | -     |
| oa:capacityAnalysis:downloadReport           | Grants permission to download a capacity optimization analysis report.                          | read         | -                           | -             | -     |
| oa:capacityAnalysis:exportReport             | Grants permission to export a capacity optimization analysis report.                            | read         | -                           | -             | -     |
| oa:capacityAnalysis:exportExpertReport       | Grants permission to export an expert analysis report on capacity optimization.                 | read         | -                           | -             | -     |
| oa:applications:list                         | Grants permission to obtain the list of architecture diagrams.                                  | read         | -                           | -             | -     |
| oa:applications:get                          | Grants permission to obtain architecture diagram details.                                       | read         | -                           | -             | -     |

| Action                                 | Description                                                                            | Access Level | Resource Type (*: Required) | Condition Key | Alias |
|----------------------------------------|----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| oa:applications:update                 | Grants permission to modify basic information about an architecture diagram.           | write        | -                           | -             | -     |
| oa:applications:delete                 | Grants permission to delete an architecture diagram.                                   | write        | -                           | -             | -     |
| oa:applications:updateView             | Grants permission to modify the settings of architecture diagram elements.             | write        | -                           | -             | -     |
| oa:applications:listServiceConfigs     | Grants permission to obtain the service configuration list of an architecture diagram. | read         | -                           | -             | -     |
| oa:applications:getResourceConfig      | Grants permission to obtain resource parsing settings of an architecture diagram.      | read         | -                           | -             | -     |
| oa:applications:updateRiskSwitchStatus | Grants permission to enable or disable risk statistics of an architecture diagram.     | write        | -                           | -             | -     |
| oa:applications:listRisks              | Grants permission to obtain the number of risks in an architecture diagram.            | read         | -                           | -             | -     |

| Action                                  | Description                                                                               | Access Level | Resource Type (*: Required) | Condition Key | Alias                       |
|-----------------------------------------|-------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------|
| oa:applications:listHistorys            | Grants permission to obtain the list of historical records of an architecture diagram.    | read         | -                           | -             | -                           |
| oa:applications:getHistory              | Grants permission to obtain the details of historical records of an architecture diagram. | read         | -                           | -             | -                           |
| oa:applications:restoreHistory          | Grants permission to restore a historical architecture diagram.                           | write        | -                           | -             | -                           |
| oa:applications:deleteHistory           | Grants permission to delete the historical records of an architecture diagram.            | write        | -                           | -             | -                           |
| oa:applications:listRecycleApplications | Grants permission to list architecture diagrams in the recycle bin.                       | read         | -                           | -             | -                           |
| oa::listSystemCesMetrics                | Grants permission to obtain Cloud Eye metrics.                                            | read         | -                           | -             | oa:system:listCesMetrics    |
| oa::listSystemCesMetricData             | Grants permission to obtain Cloud Eye metric details.                                     | read         | -                           | -             | oa:system:listCesMetricData |
| oa::getSystemConfigItem                 | Grants permission to obtain configuration items in the configuration center.              | read         | -                           | -             | oa:system:getConfigItem     |

| Action                                                 | Description                                                                                   | Access Level | Resource Type (*: Required) | Condition Key | Alias                     |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------|
| oa:capacityAnalysis:listHistoryReports                 | Grants permission to obtain the list of historical capacity optimization analysis records.    | read         | -                           | -             | -                         |
| oa:capacityAnalysis:listMetrics                        | Grants permission to obtain metrics of risky resources for capacity optimization.             | read         | -                           | -             | -                         |
| oa:capacityAnalysis:listMonitor                        | Grants permission to obtain the monitoring data of risky resources for capacity optimization. | read         | -                           | -             | -                         |
| oa::getAutoloadData                                    | Grants permission to obtain the auto-loaded data.                                             | read         | -                           | -             | oa:system:getAutoloadData |
| oa:capacityAnalysis:listResultMonitor-Data             | Grants permission to obtain the monitoring data from KEA risk analysis results.               | read         | -                           | -             | -                         |
| oa:applications:getSummary                             | Grants permission to obtain the architecture diagram summary.                                 | read         | -                           | -             | -                         |
| oa:applications:listCapacityAnalysis-SupportedServices | Grants permission to obtain supported services from the capacity optimization dashboard.      | read         | -                           | -             | -                         |



| Action                                           | Description                                                                                | Access Level | Resource Type (*: Required) | Condition Key | Alias                    |
|--------------------------------------------------|--------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------|
| oa:applications:listCapacityAnalysis-Results     | Grants permission to obtain the analysis results from the capacity optimization dashboard. | read         | -                           | -             | -                        |
| oa:applications:startAutomaticDrawAnalysis       | Grants permission to create an automatic drawing analysis task.                            | write        | -                           | -             | -                        |
| oa:applications:getAutomaticDrawAnalysisProgress | Grants permission to obtain the progress of an automatic drawing analysis task.            | read         | -                           | -             | -                        |
| oa:applications:getAutomaticDrawAnalysisResult   | Grants permission to obtain the result of an automatic drawing analysis task.              | read         | -                           | -             | -                        |
| oa:applications:getVpcFlowLogsDockingStatus      | Grants permission to obtain the interconnection status of VPC flow logs.                   | read         | -                           | -             | -                        |
| oa::listResourceGroups                           | Grants permission to obtain the resource group list.                                       | read         | -                           | -             | oa:resourceGroups:list   |
| oa::getResourceGroups                            | Grants permission to obtain resource group details.                                        | read         | -                           | -             | oa:resourceGroups:get    |
| oa::updateResourceGroups                         | Grants permission to modify a resource group.                                              | write        | -                           | -             | oa:resourceGroups:update |

| Action                               | Description                                                                  | Access Level | Resource Type (*: Required) | Condition Key | Alias                                            |
|--------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------------|
| oa::deleteResourceGroups             | Grants permission to delete a resource group.                                | write        | -                           | -             | oa:resourceGroups:delete                         |
| oa::listResourceGroupsRegions        | Grants permission to list the regions that the resource groups belong to.    | read         | -                           | -             | oa:resourceGroups:listRegions                    |
| oa::listResourceGroupsResources      | Grants permission to list the resources in a resource group.                 | read         | -                           | -             | oa:resourceGroups:listResources                  |
| oa::listEnterpriseProjectResources   | Grants permission to list the resources of an enterprise project.            | read         | -                           | -             | oa:resourceGroups:listEnterpriseProjectResources |
| oa::listServiceMetrics               | Grants permission to list metrics of a cloud service.                        | read         | -                           | -             | oa:system:listServiceMetrics                     |
| oa::listAlarmMetrics                 | Grants permission to list alarm metrics.                                     | read         | -                           | -             | oa:system:listAlarmMetrics                       |
| oa:applications:listServiceResources | Grants permission to list cloud service resources of an architecture design. | read         | -                           | -             | -                                                |
| oa:applications:saveResourceGroup    | Grants permission to save resource groups of an architecture design.         | write        | -                           | -             | -                                                |
| oa::listResourceTypes                | Grants permission to list resource types.                                    | read         | -                           | -             | oa:system:listResourceTypes                      |
| oa::listAllResourceGroups            | Grants permission to list all resource groups.                               | read         | -                           | -             | oa:resourceGroups:listAll                        |

| Action                                           | Description                                                                                         | Access Level | Resource Type (*: Required) | Condition Key | Alias                                      |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------|
| oa:applications:downloadResourceTemplate         | Grants permission to download the resource import template for an architecture design.              | read         | -                           | -             | oa:applications:downloadResourceTemplate   |
| oa:applications:importResources                  | Grants permission to import resources for an architecture design.                                   | read         | -                           | -             | -                                          |
| oa:applications:getResourcesImportResult         | Grants permission to obtain the resource import results of an architecture design.                  | read         | -                           | -             | -                                          |
| oa:applications:saveResourceGroups-Batch         | Grants permission to save resource groups in an architecture design in batches.                     | write        | -                           | -             | -                                          |
| oa:applications:getBatchSaveResourceGroupsResult | Grants permission to obtain the results for batch saving resource groups in an architecture design. | read         | -                           | -             | -                                          |
| oa::downloadResourceTemplate                     | Grants permission to download the resource import template for a resource group.                    | read         | -                           | -             | oa:resourceGroups:downloadResourceTemplate |
| oa::importResourceGroups                         | Grants permission to import resources to a resource group.                                          | read         | -                           | -             | oa:resourceGroups:importResources          |

| Action                                            | Description                                                                  | Access Level | Resource Type (*: Required) | Condition Key | Alias                                      |
|---------------------------------------------------|------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------------------|
| oa::getResourcesGroupsImportResult                | Grants permission to obtain the resource import results of a resource group. | read         | -                           | -             | oa:resourceGroups:getResourcesImportResult |
| oa:applications:startServiceRecommendAnalysis     | Grants permission to start service recommendation analysis.                  | write        | -                           | -             | -                                          |
| oa:applications:getServiceRecommendAnalysisResult | Grants permission to obtain the service recommendation analysis results.     | read         | -                           | -             | -                                          |
| oa:applications:listAttachedResources             | Grants permission to list resources associated with an architecture diagram. | read         | -                           | -             | -                                          |
| oa:applications:listNodeAttachedResources         | Grants permission to list resources corresponding to a diagram element.      | read         | -                           | -             | -                                          |
| oa:applications:downloadAttachedResources         | Grants the permission to export resources from an architecture diagram.      | write        | -                           | -             | -                                          |
| oa::getAutoloadConfigs                            | Grants permission to obtain system auto-loaded configurations                | read         | -                           | -             | oa:system:getAutoloadConfigs               |
| oa::listRiskItemsCheckReportsV4                   | Grants permission to obtain risk check reports.                              | read         | -                           | -             | oa:riskItemsCheck:listReportsV4            |

| Action                             | Description                                                                                   | Access Level | Resource Type (*: Required) | Condition Key | Alias                          |
|------------------------------------|-----------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|--------------------------------|
| oa::getResources                   | Grants permission to obtain auto-access resource data.                                        | read         | -                           | -             | oa:system:getAutoloadResources |
| oa:capacityAnalysis:getListMetrics | Grants permission to obtain metrics of risky resources for capacity optimization.             | read         | -                           | -             | -                              |
| oa:capacityAnalysis:getListMonitor | Grants permission to obtain the monitoring data of risky resources for capacity optimization. | read         | -                           | -             | -                              |

## Resources

OA does not support resource-level authorization. To allow access to OA, use a wildcard (\*) in the Resource element of the identity policy, indicating that the policy will be applied to all resources.

## Conditions

OA does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

# 3.15 Migration

## 3.15.1 Object Storage Migration Service (OMS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [service control policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that

OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [How IAM Is Different from Organizations for Access Control?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN for the Resource element in your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by OMS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by OMS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for OMS.

**Table 3-301** Actions supported by OMS

| Action              | Description                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------|---------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| oms:task:list       | Grant the permission to list migration tasks.                       | list         | task                        | -             | -     |
| oms:task:create     | Grant the permission to create a migration task.                    | write        | task                        | -             | -     |
| oms:task:get        | Grant the permission to query details about a migration task.       | read         | task                        | -             | -     |
| oms:task:delete     | Grant the permission to delete a migration task.                    | write        | task                        | -             | -     |
| oms:task:update     | Grant the permission to update a migration task.                    | write        | task                        | -             | -     |
| oms:synctask:list   | Grant the permission to list synchronization tasks.                 | list         | synctask                    | -             | -     |
| oms:synctask:create | Grant the permission to create a synchronization task.              | write        | synctask                    | -             | -     |
| oms:synctask:get    | Grant the permission to query details about a synchronization task. | read         | synctask                    | -             | -     |
| oms:synctask:delete | Grant the permission to delete a synchronization task.              | write        | synctask                    | -             | -     |

| Action                   | Description                                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------|------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| oms:synctask:statistics  | Grant the permission to query statistics about a synchronization task. | read         | synctask                    | -             | -     |
| oms:synctask:update      | Grant the permission to update a synchronization task.                 | write        | synctask                    | -             | -     |
| oms:synctask:createEvent | Grant the permission to create a synchronization event.                | write        | synctask                    | -             | -     |
| oms:taskgroup:create     | Grant the permission to create a migration task group.                 | write        | taskgroup                   | -             | -     |
| oms:taskgroup:list       | Grant the permission to list migration task groups.                    | list         | taskgroup                   | -             | -     |
| oms:taskgroup:get        | Grant the permission to query details about a migration task group.    | read         | taskgroup                   | -             | -     |
| oms:taskgroup:delete     | Grant the permission to delete a migration task group.                 | write        | taskgroup                   | -             | -     |
| oms:taskgroup:update     | Grant the permission to update a migration task group.                 | write        | taskgroup                   | -             | -     |



| Action                 | Description                                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------|-------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| oms::listObjects       | Grant the permission to list objects in a bucket.                                   | list         | -                           | -             | -     |
| oms::checkCdnInfo      | Grant the permission to check the connectivity between a bucket and CDN.            | read         | -                           | -             | -     |
| oms::listBuckets       | Grant the permission to list buckets.                                               | list         | -                           | -             | -     |
| oms::listBucketRegions | Grant the permission to query the region of a bucket.                               | list         | -                           | -             | -     |
| oms::checkBucketPrefix | Grant the permission to check whether a bucket has objects with a specified prefix. | read         | -                           | -             | -     |
| oms::listCloudRegions  | Grant the permission to query regions supported for a cloud vendor.                 | list         | -                           | -             | -     |
| oms::listCloudTypes    | Grant the permission to list supported cloud vendors.                               | list         | -                           | -             | -     |

Each API of OMS usually supports one or more actions. [Table 3-302](#) lists the actions and dependencies supported by OMS APIs.

**Table 3-302** Actions and dependencies supported by OMS APIs

| API                                                               | Action                       | Dependencies |
|-------------------------------------------------------------------|------------------------------|--------------|
| POST /v2/{project_id}/tasks/<br>batch-update                      | oms:task:update              | -            |
| GET /v2/{project_id}/tasks                                        | oms:task:list                | -            |
| POST /v2/{project_id}/tasks                                       | oms:task:create              | -            |
| GET /v2/{project_id}/tasks/<br>{task_id}                          | oms:task:get                 | -            |
| DELETE /v2/{project_id}/<br>tasks/{task_id}                       | oms:task:delete              | -            |
| POST /v2/{project_id}/tasks/<br>{task_id}/stop                    | oms:task:update              | -            |
| POST /v2/{project_id}/tasks/<br>{task_id}/start                   | oms:task:update              | -            |
| PUT /v2/{project_id}/tasks/<br>{task_id}/bandwidth-policy         | oms:task:update              | -            |
| PUT /v2/{project_id}/tasks/<br>{task_id}/access-keys              | oms:task:update              | -            |
| GET /v2/{project_id}/sync-<br>tasks                               | oms:synctask:list            | -            |
| POST /v2/{project_id}/sync-<br>tasks                              | oms:synctask:create          | -            |
| GET /v2/{project_id}/sync-<br>tasks/{sync_task_id}                | oms:synctask:get             | -            |
| DELETE /v2/{project_id}/<br>sync-tasks/{sync_task_id}             | oms:synctask:delete          | -            |
| GET /v2/{project_id}/sync-<br>tasks/{sync_task_id}/<br>statistics | oms:synctask:statistic<br>s  | -            |
| POST /v2/{project_id}/sync-<br>tasks/{sync_task_id}/stop          | oms:synctask:update          | -            |
| POST /v2/{project_id}/sync-<br>tasks/{sync_task_id}/start         | oms:synctask:update          | -            |
| POST /v2/{project_id}/sync-<br>tasks/{sync_task_id}/events        | oms:synctask:createE<br>vent | -            |
| POST /v2/{project_id}/<br>taskgroups                              | oms:taskgroup:create         | -            |
| GET /v2/{project_id}/<br>taskgroups                               | oms:taskgroup:list           | -            |

| API                                                  | Action                 | Dependencies |
|------------------------------------------------------|------------------------|--------------|
| GET /v2/{project_id}/taskgroups/{group_id}           | oms:taskgroup:get      | -            |
| DELETE /v2/{project_id}/taskgroups/{group_id}        | oms:taskgroup:delete   | -            |
| PUT /v2/{project_id}/taskgroups/{group_id}/stop      | oms:taskgroup:update   | -            |
| PUT /v2/{project_id}/taskgroups/{group_id}/start     | oms:taskgroup:update   | -            |
| PUT /v2/{project_id}/taskgroups/{group_id}/retry     | oms:taskgroup:update   | -            |
| PUT /v2/{project_id}/taskgroups/{group_id}/update    | oms:taskgroup:update   | -            |
| POST /v2/{project_id}/objectstorage/buckets/objects  | oms::listObjects       | -            |
| POST /v2/{project_id}/objectstorage/buckets/cdn-info | oms::checkCdnInfo      | -            |
| POST /v2/{project_id}/objectstorage/buckets          | oms::listBuckets       | -            |
| POST /v2/{project_id}/objectstorage/buckets/regions  | oms::listBucketRegions | -            |
| POST /v2/{project_id}/objectstorage/buckets/prefix   | oms::checkBucketPrefix | -            |
| GET /v2/{project_id}/objectstorage/data-center       | oms::listCloudRegions  | -            |
| GET /v2/{project_id}/objectstorage/cloud-type        | oms::listCloudTypes    | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-303](#), a resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in a policy to define resource types.

The following table lists the resource types that you can specify in identity policy statements for OMS.

**Table 3-303** Resource types supported by OMS

| Resource Type | URN                                              |
|---------------|--------------------------------------------------|
| Task          | oms:<region>:<account-id>:task:*                 |
|               | oms:<region>:<account-id>:task:<task-id>         |
| SyncTask      | oms:<region>:<account-id>:synctask:*             |
|               | oms:<region>:<account-id>:synctask:<synctask-id> |
| TaskGroup     | oms:<region>:<account-id>:taskgroup:*            |
|               | oms:<region>:<account-id>:taskgroup:*            |

**NOTICE**

Currently, synchronization task APIs are available only in CN South-Guangzhou-InvitationOnly, CN North-Beijing4, and CN East-Shanghai1.

## Conditions

OMS does not support service-specific condition keys in identity policies.

It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.15.2 Server Migration Service (SMS)

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [service control policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs just determine what permissions are available for that member account or those member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM is different from Organizations for access control, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).

- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify a URN for the Resource element in your identity policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by SMS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by SMS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for SMS.

**Table 3-304** Actions supported by SMS

| Action            | Description                          | Access Level | Resource Type (*: required) | Condition Key | Alias                  |
|-------------------|--------------------------------------|--------------|-----------------------------|---------------|------------------------|
| sms:template:list | Grants permission to list templates. | list         | template                    | -             | sms:server:queryServer |

| Action                         | Description                                                          | Access Level | Resource Type (*: required) | Condition Key         | Alias                      |
|--------------------------------|----------------------------------------------------------------------|--------------|-----------------------------|-----------------------|----------------------------|
| sms:template:create            | Grants permission to create a template.                              | write        | template                    | -                     | sms:server:migrationServer |
| sms:template:batchDelete       | Grants permission to batch delete templates.                         | write        | template                    | -                     | -                          |
| sms:template:get               | Grants permission to query the information about a template.         | read         | template                    | -                     | sms:server:queryServer     |
| sms:template:update            | Grants permission to modify a template.                              | write        | template                    | -                     | sms:server:migrationServer |
| sms:template:getTargetPassword | Grants permission to query the target server password in a template. | read         | template                    | -                     | sms:server:queryServer     |
| sms:template:delete            | Grants permission to delete a template.                              | write        | template                    | -                     | sms:server:migrationServer |
| sms:server:listErrors          | Grants permission to list failed source servers.                     | list         | server                      | -                     | server:queryServer         |
| sms:server:list                | Grants permission to list source servers.                            | list         | server                      | g:EnterpriseProjectId | sms:server:queryServer     |
| sms:server:register            | Grants permission to register a source server with SMS.              | write        | server                      | g:EnterpriseProjectId | sms:server:registerServer  |

| Action                    | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                      |
|---------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------|
| sms:server:batchDelete    | Grants permission to batch delete source server records.                   | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | -                          |
| sms:server:get            | Grants permission to query the details about a source server.              | read         | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:queryServer     |
| sms:server:update         | Grants permission to modify a source server name.                          | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |
| sms:server:delete         | Grants permission to delete a source server record.                        | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |
| sms:server:updateDiskInfo | Grants permission to update disk information.                              | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:registerServer  |
| sms:server:overview       | Grants permission to obtain the summary of source servers.                 | read         | server                      | -                                     | sms:server:queryServer     |
| sms:server:updateState    | Grants permission to update the migration task status for a source server. | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |
| sms:server:listTask       | Grants permission to list migration tasks.                                 | list         | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:queryServer     |
| sms:server:createTask     | Grants permission to create a migration task.                              | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |

| Action                        | Description                                                    | Access Level | Resource Type (*: required) | Condition Key                         | Alias                      |
|-------------------------------|----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------|
| sms:server:batchDeleteTask    | Grants permission to batch delete migration tasks.             | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | -                          |
| sms:server:getTask            | Grants permission to query the details about a migration task. | read         | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:queryServer     |
| sms:server:updateTask         | Grants permission to update a migration task.                  | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |
| sms:server:deleteTask         | Grants permission to delete a migration task.                  | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:deleteTask      |
| sms:server:manageTask         | Grants permission to manage migration tasks.                   | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |
| sms:server:updateTaskProgress | Grants permission to report the migration progress and rate.   | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |
| sms:server:unlock             | Grants permission to unlock a target server.                   | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | -                          |
| sms:server:collectLog         | Grants permission to upload migration task logs.               | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |
| sms:server:getTaskPassphrase  | Grants permission to query a certificate passphrase.           | read         | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:queryServer     |



| Action                          | Description                                                                | Access Level | Resource Type (*: required) | Condition Key                         | Alias                        |
|---------------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|------------------------------|
| sms:server:checkNetwork         | Grants permission to check NICs and security groups.                       | read         | server                      | -                                     | -                            |
| sms:server:getTaskSpeedLimit    | Grants permission to query the traffic limiting rules of a migration task. | read         | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:getTaskSpeedLimit |
| sms:server:updateTaskSpeedLimit | Grants permission to set traffic limiting rules for a migration task.      | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer   |
| sms:server:getCommand           | Grants permission to obtain commands from SMS.                             | read         | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer   |
| sms:server:updateCommandResult  | Grants permission to report command execution results to SMS.              | write        | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer   |
| sms:server:getCert              | Grants permission to obtain an SSL certificate and private key.            | read         | server                      | <a href="#">g:EnterpriseProjectId</a> | sms:server:queryServer       |
| sms:migproject:list             | Grants permission to list migration projects.                              | list         | migproject                  | -                                     | sms:server:queryServer       |
| sms:migproject:create           | Grants permission to create a migration project.                           | write        | migproject                  | -                                     | sms:server:migrationServer   |

| Action                            | Description                                                                      | Access Level | Resource Type (*: required) | Condition Key                | Alias                      |
|-----------------------------------|----------------------------------------------------------------------------------|--------------|-----------------------------|------------------------------|----------------------------|
| sms:migproject:get                | Grants permission to query details about a migration project.                    | read         | migproject                  | -                            | sms:server:queryServer     |
| sms:migproject:update             | Grants permission to update a migration project.                                 | write        | migproject                  | -                            | sms:server:migrationServer |
| sms:migproject:delete             | Grants permission to delete a migration project.                                 | write        | migproject                  | -                            | sms:server:migrationServer |
| sms:migproject:update             | Grants permission to change the default migration project.                       | write        | migproject                  | -                            | sms:server:migrationServer |
| sms::getConfig                    | Grants permission to obtain Agent configuration information.                     | read         | -                           | -                            | sms:server:queryServer     |
| sms:server:updateNetworkCheckInfo | Grants permission to update network measurement information.                     | write        | task                        | <b>g:EnterpriseProjectId</b> | sms:server:migrationServer |
| sms:server:getTaskConfig          | Grants permission to query the settings of advanced migration options of a task. | read         | task                        | <b>g:EnterpriseProjectId</b> | sms:server:queryServer     |

| Action                      | Description                                                     | Access Level | Resource Type (*: required) | Condition Key                         | Alias                      |
|-----------------------------|-----------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|----------------------------|
| sms:server:updateTaskConfig | Grants permission to set advanced migration options for a task. | write        | task                        | <a href="#">g:EnterpriseProjectId</a> | sms:server:migrationServer |

Each API of SMS usually supports one or more actions. [Table 3-305](#) lists the supported actions and dependencies.

**Table 3-305** Actions and dependencies supported by SMS APIs

| API                                       | Action                         | Dependencies |
|-------------------------------------------|--------------------------------|--------------|
| GET /v3/vm/templates                      | sms:template:list              | -            |
| POST /v3/vm/templates                     | sms:template:create            | -            |
| POST /v3/vm/templates/delete              | sms:template:batchDelete       | -            |
| GET /v3/vm/templates/{id}                 | sms:template:get               | -            |
| PUT /v3/vm/templates/{id}                 | sms:template:update            | -            |
| GET /v3/vm/templates/{id}/target-password | sms:template:getTargetPassword | -            |
| DELETE /v3/vm/templates/{id}              | sms:template:delete            | -            |
| GET /v3/errors                            | sms:server:listErrors          | -            |
| GET /v3/sources                           | sms:server:list                | -            |
| POST /v3/sources                          | sms:server:register            | -            |

| API                                     | Action                    | Dependencies                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v3/sources/delete                 | sms:server:batchDelete    | <ul style="list-style-type: none"> <li>ecs:cloudServers:showServer</li> <li>ecs:cloudServers:attach</li> <li>evs:volumes:use</li> <li>ecs:cloudServers:stop</li> <li>ecs:cloudServers:start</li> <li>ecs:cloudServers:detachVolume</li> <li>evs:volumes:delete</li> <li>evs:snapshots:delete</li> <li>evs:volumes:get</li> </ul> |
| GET /v3/sources/{source_id}             | sms:server:get            | -                                                                                                                                                                                                                                                                                                                                |
| PUT /v3/sources/{source_id}             | sms:server:update         | -                                                                                                                                                                                                                                                                                                                                |
| DELETE /v3/sources/{source_id}          | sms:server:delete         | <ul style="list-style-type: none"> <li>ecs:cloudServers:showServer</li> <li>ecs:cloudServers:attach</li> <li>evs:volumes:use</li> <li>ecs:cloudServers:stop</li> <li>ecs:cloudServers:start</li> <li>ecs:cloudServers:detachVolume</li> <li>evs:volumes:delete</li> <li>evs:snapshots:delete</li> <li>evs:volumes:get</li> </ul> |
| PUT /v3/sources/{source_id}/diskinfo    | sms:server:updateDiskInfo | -                                                                                                                                                                                                                                                                                                                                |
| GET /v3/sources/overview                | sms:server:overview       | -                                                                                                                                                                                                                                                                                                                                |
| PUT /v3/sources/{source_id}/changestate | sms:server:updateState    | -                                                                                                                                                                                                                                                                                                                                |
| GET /v3/tasks                           | sms:server:listTask       | -                                                                                                                                                                                                                                                                                                                                |
| POST /v3/tasks                          | sms:server:createTask     | -                                                                                                                                                                                                                                                                                                                                |

| API                                | Action                        | Dependencies                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| POST /v3/tasks/delete              | sms:server:batchDeleteTask    | <ul style="list-style-type: none"> <li>ecs:cloudServers:showServer</li> <li>ecs:cloudServers:attach</li> <li>evs:volumes:use</li> <li>ecs:cloudServers:stop</li> <li>ecs:cloudServers:start</li> <li>ecs:cloudServers:detachVolume</li> <li>evs:volumes:delete</li> <li>evs:snapshots:delete</li> <li>evs:volumes:get</li> </ul> |
| GET /v3/tasks/{task_id}            | sms:server:getTask            | -                                                                                                                                                                                                                                                                                                                                |
| PUT /v3/tasks/{task_id}            | sms:server:updateTask         | -                                                                                                                                                                                                                                                                                                                                |
| DELETE /v3/tasks/{task_id}         | sms:server:deleteTask         | <ul style="list-style-type: none"> <li>ecs:cloudServers:showServer</li> <li>ecs:cloudServers:attach</li> <li>evs:volumes:use</li> <li>ecs:cloudServers:stop</li> <li>ecs:cloudServers:start</li> <li>ecs:cloudServers:detachVolume</li> <li>evs:volumes:delete</li> <li>evs:snapshots:delete</li> <li>evs:volumes:get</li> </ul> |
| POST /v3/tasks/{task_id}/action    | sms:server:manageTask         | -                                                                                                                                                                                                                                                                                                                                |
| PUT /v3/tasks/{task_id}/progress   | sms:server:updateTaskProgress | -                                                                                                                                                                                                                                                                                                                                |
| POST /v3/tasks/{task_id}/unlock    | sms:server:unlock             | -                                                                                                                                                                                                                                                                                                                                |
| POST /v3/tasks/{task_id}/log       | sms:server:collectLog         | -                                                                                                                                                                                                                                                                                                                                |
| GET /v3/tasks/{task_id}/passphrase | sms:server:getTaskPassphrase  | -                                                                                                                                                                                                                                                                                                                                |

| API                                                          | Action                            | Dependencies |
|--------------------------------------------------------------|-----------------------------------|--------------|
| GET /v3/tasks/{t_project_id}/networkacl/{t_network_id}/check | sms:server:checkNetwork           | -            |
| GET /v3/tasks/{task_id}/speed-limit                          | sms:server:getTaskSpeedLimit      | -            |
| POST /v3/tasks/{task_id}/speed-limit                         | sms:server:updateTaskSpeedLimit   | -            |
| GET /v3/sources/{server_id}/command                          | sms:server:getCommand             | -            |
| POST /v3/sources/{server_id}/command_result                  | sms:server:updateCommandResult    | -            |
| GET /v3/tasks/{task_id}/certkey                              | sms:server:getCert                | -            |
| GET /v3/migprojects                                          | sms:migproject:list               | -            |
| POST /v3/migprojects                                         | sms:migproject:create             | -            |
| GET /v3/migprojects/{mig_project_id}                         | sms:migproject:get                | -            |
| PUT /v3/migprojects/{mig_project_id}                         | sms:migproject:update             | -            |
| DELETE /v3/migprojects/{mig_project_id}                      | sms:migproject:delete             | -            |
| PUT /v3/migprojects/{mig_project_id}/default                 | sms:migproject:update             | -            |
| GET /v3/config                                               | sms::getConfig                    | -            |
| POST /v3/{task_id}/update-network-check-info                 | sms:server:updateNetworkCheckInfo | -            |
| POST /v3/tasks/{task_id}/configuration-setting               | sms:server:updateTaskConfig       | -            |

## Resources

A resource type indicates the resources that an identity policy applies to. If you specify a resource type for any action in [Table 3-306](#), a resource URN must be specified in the identity policy statements using that action, and the identity policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (\*) and the identity policy applies to all resources. You can also set condition keys in a policy to define resource types.

The following table lists the resource types that you can specify in identity policy statements for SMS.

**Table 3-306** Resource types supported by SMS

| Resource Type | URN                                          |
|---------------|----------------------------------------------|
| server        | sms::<account-id>:server:*                   |
|               | sms::<account-id>:server:<server-id>         |
| Task          | sms::<account-id>:task:*                     |
|               | sms::<account-id>:task:<task-id>             |
| template      | sms::<account-id>:template:*                 |
|               | sms::<account-id>:template:<template-id>     |
| migproject    | sms::<account-id>:migproject:*               |
|               | sms::<account-id>:migproject:<migproject-id> |

## Conditions

SMS does not support service-specific condition keys in identity policies.

It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

## 3.16 Customer Services

### 3.16.1 Billing Center

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [service control policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences in Access Control Between IAM and Organizations?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to create an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to create a custom SCP, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (such as **list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resources types defined by Billing Center, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Billing Center, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Billing Center.



**Table 3-307** Actions supported by Billing Center

| Action                          | Permissions                                                                                                                 | Access Level | Resource Type (*: required) | Condition Key                         | Alias |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------------------------------|-------|
| billing:balance:update          | Grants permission to withdraw money, top up the account, make payments, and enable balance alerting.                        | write        | -                           | -                                     | -     |
| billing:balance:view            | Grants permission to view account statements, payment records, expenditure quotas, account adjustment records, and arrears. | list         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| billing:balance:export          | Grants permission to export transaction and payment records.                                                                | read         | -                           | -                                     | -     |
| billing:bill:update             | Grants permission to update bills.                                                                                          | write        | -                           | -                                     | -     |
| billing:bill:view               | Grants permission to view bills, expenditures of the current month, and expenditure trends.                                 | list         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| billing:bill:export             | Grants permission to export the bill summary.                                                                               | read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| billing:billDetail:update       | Grants permission to update bill details.                                                                                   | write        | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| billing:billDetail:view         | Grants permission to view bill details.                                                                                     | read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| billing:billDetail:export       | Grants permission to export bill details.                                                                                   | read         | -                           | <a href="#">g:EnterpriseProjectId</a> | -     |
| billing:resourcePackages:view   | Grants permission to view resource packages, remaining usage, and usage details, and to export resource usage details.      | list         | -                           | -                                     | -     |
| billing:resourcePackages:update | Grants permission to set alerts for remaining usage of resource packages.                                                   | write        | -                           | -                                     | -     |

| Action                           | Permissions                                                                                                                                         | Access Level | Resource Type (*: required) | Condition Key         | Alias |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|-----------------------|-------|
| billing:contract:update          | Grants permission to view offline contracts.                                                                                                        | write        | -                           | -                     | -     |
| billing:coupon:view              | Grants permission to view and activate coupons.                                                                                                     | read         | -                           | -                     | -     |
| billing:contract:viewDiscount    | Grants permission to view commercial discounts.                                                                                                     | read         | -                           | -                     | -     |
| billing:invoice:manage           | Grants permission to manage invoices.                                                                                                               | write        | -                           | -                     | -     |
| billing:invoice:view             | Grants permission to view invoice history and details.                                                                                              | read         | -                           | -                     | -     |
| billing:invoice:export           | Grants permission to export invoice information and download invoices.                                                                              | read         | -                           | -                     | -     |
| billing:order:pay                | Grants permission to pay for orders.                                                                                                                | write        | -                           | g:EnterpriseProjectId | -     |
| billing:order:view               | Grants permission to view order information and pay-per-usage resource packages.                                                                    | list         | -                           | g:EnterpriseProjectId | -     |
| billing:subscription:renew       | Grants permission to renew resources, enable auto-renewal, set expiration policies, and change the billing mode from pay-per-use to yearly/monthly. | write        | -                           | g:EnterpriseProjectId | -     |
| billing:subscription:view        | Grants permission to view renewals and query resources that can be changed from pay-per-use to yearly/monthly.                                      | list         | -                           | g:EnterpriseProjectId | -     |
| billing:subscription:unsubscribe | Grants permission to view resources that can be unsubscribed from and have been unsubscribed from.                                                  | write        | -                           | g:EnterpriseProjectId | -     |
| billing:consumption:view         | Grants permission to view expenditure breakdowns by enterprise project.                                                                             | read         | -                           | -                     | -     |
| billing::activeEPFinance         | Grants permission to enable or disable EPS.                                                                                                         | write        | -                           | -                     | -     |

| Action                          | Permissions                                                                             | Access Level | Resource Type (*: required) | Condition Key | Alias |
|---------------------------------|-----------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| billing::activeEPFundQuota      | Grants permission to enable or disable the fund quota function for enterprise projects. | write        | -                           | -             | -     |
| billing::viewEPFundQuota        | Grants permission to query the fund quota of an enterprise project.                     | read         | -                           | -             | -     |
| billing::updateEPFundQuota      | Grants permission to modify the fund quota of an enterprise project.                    | write        | -                           | -             | -     |
| billing::listEPFundQuotaHistory | Grants permission to view the fund quota adjustment records of enterprise projects.     | read         | -                           | -             | -     |
| billing::updateEPGroup          | Grants permission to modify enterprise project groups.                                  | write        | -                           | -             | -     |
| billing::viewEPGroup            | Grants permission to view enterprise project groups.                                    | read         | -                           | -             | -     |

For details about the relationship between Billing Center APIs and actions, see [Customer Operations](#).

## Resources

Billing Center does not support resource-level authorization. To allow access to Billing Center, use a wildcard (\*) in the Resource element of the identity policy, indicating that the identity policy will be applied to all resources.

## Conditions

### Condition Key

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).

- Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **BILLING:**) only apply to operations of the specified service. For details, see [Table 3-308](#).
- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.
- A condition operator, a condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see [Operators](#).

### Service-specific Condition Keys Supported by Billing Center

The following table lists the condition keys that you can define in identity policies for Billing Center. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-308** Service-specific condition keys supported by Billing Center

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                       |
|--------------------------------|--------|-------------------------------|-----------------------------------------------------------------------------------|
| billing:cloudServiceType       | string | Multivalued                   | Filter access based on the cloud service type specified in the request parameter. |

### Condition Key Examples

billing:cloudServiceType

Example: Only cloud service resources of the `hws.service.type.ebs` type can be unsubscribed from.

```
{  "Version": "5.0",  "Statement": [{    "Effect": "Allow",    "Action": "billing:subscription:unsubscribe",    "Condition": {      "ForAnyValue:StringEquals": {        "billing:cloudServiceType": "hws.service.type.ebs"      }    }  } ]}
```

## 3.16.2 Cost Center

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [service control policies \(SCPs\)](#) for access control.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences Between IAM Policies and Organizations SCPs?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP policy, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (such as **list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in a policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by Cost Center, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Cost Center, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Cost Center.

**Table 3-309** Actions supported by Cost Center

| Action                                | Description                                                                                           | Access Level | Resource Type (*: required) | Condition Key | Alias                   |
|---------------------------------------|-------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------|
| costCenter:accessAccount:view         | Grants permission to view access accounts.<br>(Only available on the Chinese mainland website.)       | read         | -                           | -             | bss:accessAccount:view  |
| costCenter:costAnalysis:listCosts     | Grants permission to view cost analyses.                                                              | read         | -                           | -             | bss:costanalysis:view   |
| costCenter:costAnalysis:configReport  | Grants permission to manage cost reports, including creating, modifying, and deleting custom reports. | write        | -                           | -             | bss:costreport:update   |
| costCenter:costAnalysis:listReports   | Grants permission to view a list of cost reports.                                                     | read         | -                           | -             | bss:costreport:view     |
| costCenter:costDetail:listCostDetails | Grants permission to view cost details.                                                               | read         | -                           | -             | bss:costanalysis:view   |
| costCenter:budget:configBudget        | Grants permission to manage budgets, including creating, modifying, and deleting budgets.             | write        | -                           | -             | bss:budget:update       |
| costCenter:budget:viewBudget          | Grants permission to view budget information, including the budget list and budget details.           | read         | -                           | -             | bss:budget:view         |
| costCenter:budget:deleteBudgetReport  | Grants permission to delete a budget report.                                                          | write        | -                           | -             | bss:budgetreport:delete |
| costCenter:budget:configBudgetReport  | Grants permission to add and modify a budget report.                                                  | write        | -                           | -             | bss:budgetreport:update |
| costCenter:budget:viewBudgetReport    | Grants permission to view budget reports, including the report list and details.                      | read         | -                           | -             | bss:budgetreport:view   |

| Action                                                     | Description                                                                                       | Access Level | Resource Type (*: required) | Condition Key | Alias                         |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------|
| costCenter:costAnomalyDetection:deleteMonitor              | Grants permission to delete a cost monitor.                                                       | write        | -                           | -             | bss:monitor:delete            |
| costCenter:costAnomalyDetection:configMonitor              | Grants permission to add and edit a cost monitor.                                                 | write        | -                           | -             | bss:monitor:update            |
| costCenter:costAnomalyDetection:viewMonitor                | Grants permission to view cost monitors and anomalies.                                            | read         | -                           | -             | bss:monitor:view              |
| costCenter:costAnomalyDetection:configMonitorAlert         | Grants permission to configure alerting for cost anomalies.                                       | write        | -                           | -             | bss:monitor:alert:update      |
| costCenter:costAnomalyDetection:viewMonitorAlert           | Grants permission to view cost anomaly alerts.                                                    | read         | -                           | -             | bss:monitor:alert:view        |
| costCenter:recommendation:viewRecommendationSummary        | Grants permission to view the summary of cost optimization recommendations.                       | read         | -                           | -             | bss:recommendation:view       |
| costCenter:recommendation:viewRecommendationSubscription   | Grants permission to query subscriptions to cost optimization recommendations.                    | read         | -                           | -             | bss:recommendation:sub:view   |
| costCenter:recommendation:configRecommendationSubscription | Grants permission to configure or delete subscriptions to cost optimization recommendations.      | write        | -                           | -             | bss:recommendation:sub:update |
| costCenter:recommendation:viewYearlyMonthlyRecommendation  | Grants permission to view the cost optimization option of changing pay-per-use to yearly/monthly. | read         | -                           | -             | bss:costoptimization:view     |

| Action                                                       | Description                                                                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias                           |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------|
| costCenter:recommendation:viewResourcePkgRecommendation      | Grants permission to view resource package purchase recommendations.<br>(Only available on the Chinese mainland website.)       | read         | -                           | -             | bss:packageRecommendation:view  |
| costCenter:recommendation:viewResourceOptimizeRecommendation | Grants permission to view optimization recommendations for idle resources.<br>(Only available on the Chinese mainland website.) | read         | -                           | -             | bss:instanceOptimization:view   |
| costCenter:recommendation:configPreference                   | Grants permission to define idle resource identifying rules.<br>(Only available on the Chinese mainland website.)               | write        | -                           | -             | bss:instanceOptimization:update |
| costCenter:costTag:updateStatus                              | Grants permission to activate or deactivate cost tags.                                                                          | write        | -                           | -             | bss:costtag:update              |
| costCenter:costTag:listCostTags                              | Grants permission to view cost tags.                                                                                            | read         | -                           | -             | bss:costtag:view                |
| costCenter:costCategory:deleteCostCategory                   | Grants permission to delete a cost category.                                                                                    | write        | -                           | -             | bss:costunit:delete             |
| costCenter:costCategory:configCostCategory                   | Grants permission to configure cost categories, including creating and editing cost categories.                                 | write        | -                           | -             | bss:costunit:update             |
| costCenter:resourceCategory:view                             | Grants permission to view the multi-level cost directory.<br>(Only available on the Chinese mainland website.)                  | read         | -                           | -             | bss:resourceCategory:view       |



| Action                                                   | Description                                                                                                                               | Access Level | Resource Type (*: required) | Condition Key | Alias                               |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------------------------------------|
| costCenter:costCategory:viewCostCategory                 | Grants permission to view cost category information, including the cost category list and the details of each cost category.              | read         | -                           | -             | bss:costunit:view                   |
| costCenter:cloudIntelligenceDashboard:view               | Grants permission to view the cloud intelligence dashboard.<br>(Only available on the Chinese mainland website.)                          | read         | -                           | -             | bss:cloudIntelligenceDashboard:view |
| costCenter:uniCostAnalysis:listCosts                     | Grants permission to view multi-cloud cost analyses.<br>(Only available on the Chinese mainland website.)                                 | read         | -                           | -             | bss:unicostanalysis:view            |
| costCenter:resourcePackage:viewResourcePkgAnalysis       | Grants permission to view the analysis of resource package utilization and coverage.<br>(Only available on the Chinese mainland website.) | read         | -                           | -             | bss:resourcepackage:view            |
| costCenter:savingsPlans:viewSavingsPlansAnalysis         | Grants permission to view the analysis of savings plan utilization and coverage.                                                          | read         | -                           | -             | bss:savingsplan:analysis            |
| costCenter:reserveInstance:viewRIAnalysis                | Grants permission to view the analysis of reserved instance utilization and coverage.                                                     | read         | -                           | -             | bss:riusageanalysis:view            |
| costCenter:savingsPlans:viewSavingsPlans                 | Grants permission to view savings plans.                                                                                                  | read         | -                           | -             | bss:savingsplan:view                |
| costCenter:recommendation:viewSavingsPlansRecommendation | Grants permission to view savings plans purchase recommendations.                                                                         | read         | -                           | -             | bss:savingsplan:suggest             |

| Action                                       | Description                                                                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias                                 |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|---------------------------------------|
| costCenter::updateCostConfig                 | Grants permission to enable Cost Center functions.                                                                         | write        | -                           | -             | bss:costpreferences:update            |
| costCenter:preference:delete                 | Grants permission to disable Cost Center functions.                                                                        | write        | -                           | -             | bss:costpreferences:delete            |
| costCenter:costdetailreport:viewReportTask   | Grants permission to view the task list for exporting cost details to OBS.                                                 | read         | -                           | -             | bss:costdetailreport:view             |
| costCenter:costdetailreport:configReportTask | Grants permission to create, modify, or delete the tasks of exporting cost details to OBS.                                 | write        | -                           | -             | bss:costdetailreport:update           |
| costCenter:resourcePackage:viewLowUsageAlert | Grants permission to view alerts for underutilized resource packages.<br>(Only available on the Chinese mainland website.) | read         | -                           | -             | bss:resourcepackage:viewlowusagealert |
| costCenter:helper:listCostAllocations        | Grants permission to view the percentage of allocated costs.                                                               | list         | -                           | -             | bss:costhelper:viewcostallocations    |
| costCenter:helper:viewCostRating             | Grants permission to view cost allocation maturity rating.                                                                 | read         | -                           | -             | bss:costhelper:viewcostrating         |
| costCenter:resourceCategory:config           | Grants permission to configure the multi-level cost directory.<br>(Only available on the Chinese mainland website.)        | write        | -                           | -             | bss:resourceCategory:config           |
| costCenter:accessAccount:config              | Grants permission to configure access accounts.<br>(Only available on the Chinese mainland website.)                       | write        | -                           | -             | bss:accessAccount:config              |

| Action                                          | Description                                                                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias                                   |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-----------------------------------------|
| costCenter:resourcePackage:configLowUsageAlert  | Grants permission to configure alerts for underutilized resource packages.<br>(Only available on the Chinese mainland website.) | write        | -                           | -             | bss:resourcepackage:configlowusagealert |
| costCenter:costAnomalyDetection:provideFeedback | Grants permission to provide feedback on cost anomalies.                                                                        | read         | -                           | -             | -                                       |

For details about the relationship between Cost Center APIs and actions, see [Customer Operations](#).

## Resources

Cost Center does not support resource-level authorization. To allow access to Cost Center, use a wildcard (\*) in the Resource element of the identity policy, indicating that the policy will be applied to all resources.

## Conditions

Cost Center does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.16.3 My Account

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [service control policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to an entity. They only set the permissions boundary for the entity. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences Between IAM Policies and Organizations SCPs?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP policy, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (such as **list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.
- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by My Account, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for My Account.

**Table 3-310** Actions supported by My Account

| Action                     | Description                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------|----------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| account:accountinfo:update | Update account information, including basic information and preferences.   | write        | -                           | -             | -     |
| account:cps:view           | View the promotion data of Recommendations and Rebates by cloud promoters. | read         | -                           | -             | -     |
| account:cps:update         | Join the reward promotion program.                                         | write        | -                           | -             | -     |
| account:privilege:view     | View my privileges and prizes.                                             | read         | -                           | -             | -     |

## Resources

My Account does not support resource-specific permission control in identity policies. If you want to allow access to My Account, use the wildcard (\*) for the Resource element to apply identity policies to all resources.

## Conditions

My Account does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).

### 3.16.4 Enterprise Center

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM policies, you can use [service control policies \(SCPs\)](#) provided by [Organizations](#) for access control.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to a member account or an organizational unit (OU), they do not directly grant permissions to that member account or OU. Instead, the SCPs just determine what permissions are available for that member account or the member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences Between IAM Policies and Organizations SCPs?](#)

This section describes the elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP policy, see [Creating an SCP](#).

## Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions, and you must specify all resources ("\*") in your identity policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.
- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.
  - If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about the condition keys defined by Enterprise Center, see [Conditions](#).

- The **Alias** column lists the policy actions that can be configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements for Enterprise Center.

**Table 3-311** Actions supported by Enterprise Center

| Action                                        | Description                                                                     | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-----------------------------------------------|---------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| businessUnitCenter::active                    | Grants permission to enable and disable Enterprise Center.                      | write        | -                           | -             | -     |
| businessUnitCenter:bill:update                | Grants permission to manage bills for enterprise members.                       | write        | -                           | -             | -     |
| businessUnitCenter:bill:view                  | Grants permission to view bills of member accounts.                             | read         | -                           | -             | -     |
| businessUnitCenter:billDetail:update          | Grants permission to perform operations on bill details for enterprise members. | write        | -                           | -             | -     |
| businessUnitCenter:billDetail:view            | Grants permission to view bill details of member accounts.                      | read         | -                           | -             | -     |
| businessUnitCenter:businessUnitFinance:update | Grants permission to modify organization accounting information.                | write        | -                           | -             | -     |
| businessUnitCenter:businessUnitFinance:view   | Grants permission to view organization accounting information.                  | read         | -                           | -             | -     |

| Action                                       | Description                                            | Access Level | Resource Type (*: required) | Condition Key | Alias |
|----------------------------------------------|--------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| businessUnitCenter:businessUnit:update       | Grants permission to modify organizations and accounts | write        | -                           | -             | -     |
| businessUnitCenter:businessUnit:view         | Grants permission to view organizations and accounts   | read         | -                           | -             | -     |
| businessUnitCenter:businessUnitBudget:update | Grants permission to update organization budgets       | write        | -                           | -             | -     |
| businessUnitCenter:businessUnitBudget:view   | Grants permission to view organization budgets         | read         | -                           | -             | -     |
| businessUnitCenter:businessUnitPolicy:update | Grants permission to modify organization policies.     | write        | -                           | -             | -     |

For details about the relationship between Enterprise Center APIs and actions, see [Customer Operations](#).

## Resource Type (\*: required)

Enterprise Center does not support resource-specific permission control in identity policies. If you want to allow access to Enterprise Center, use the wildcard (\*) for the Resource element to apply identity policies to all resources.

## Conditions

Enterprise Center does not support service-specific condition keys in identity policies. It can only use global condition keys applicable to all services. For details, see [Global Condition Keys](#).



### 3.16.5 Customer Operation Capabilities

IAM provides system-defined identity policies to define common actions supported by cloud services. You can also create custom identity policies using the actions supported by cloud services for more refined access control.

In addition to IAM, the [Organizations](#) service also provides [Service Control Policies \(SCPs\)](#) to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permissions boundary for the principal. When SCPs are attached to an organizational unit (OU) or a member account, the SCPs do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or those member accounts under that OU. The granted IAM permissions can be applied only if they are allowed by the SCPs.

To learn more about how IAM policies are different from Organizations SCPs, see [What Are the Differences Between IAM Policies and Organizations SCPs?](#)

This section describes the authorization elements used by IAM custom identity policies and Organizations SCPs. The elements include actions, resources, and conditions.

- For details about how to use these elements to edit an IAM custom identity policy, see [Creating a Custom Identity Policy](#).
- For details about how to use these elements to edit a custom SCP policy, see [Creating an SCP](#).

#### Actions

Actions are specific operations that are allowed or denied in an identity policy.

- The **Access Level** column describes how the action is classified (**list**, **read**, or **write**). This classification helps you understand the level of access that an action grants when you use it in an identity policy.
- The **Resource Type** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (\*) to indicate all resource types. If this column is empty (-), the action does not support resource-level permissions and you must specify all resources ("\*") in your policy statements.
  - If this column includes a resource type, you must specify the URN in the Resource element of your policy statements.
  - Required resources are marked with asterisks (\*) in the table. If you specify a resource in a statement using this action, then it must be of this type.

For details about the resource types defined by BSS, see [Resources](#).

- The **Condition Key** column contains keys that you can specify in the Condition element of an identity policy statement.
  - If the **Resource Type** column has values for an action, the condition key takes effect only for the listed resource types.
  - If the **Resource Type** column is empty (-) for an action, the condition key takes effect for all resources that action supports.

- If the **Condition Key** column is empty (-) for an action, the action does not support any condition keys.

For details about condition keys defined by BSS, see [Conditions](#).

- The **Alias** column lists the policy actions that are configured in identity policies. With these actions, you can use APIs for policy-based authorization. For details, see [Policies and Identity Policies](#).

The following table lists the actions that you can define in identity policy statements.

 **NOTE**

The **billing:contract:viewDiscount** permission code only affects the discount information returned in the response, but it does not affect the API call. When there is no permission, the API can still be accessed normally, but it will not return the discount information.

**Table 3-312** Actions supported by BSS

| Action                        | Description                                                                                                                                | Access Level | Resource Type (*: required) | Condition Key | Alias |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| billing:contract:viewDiscount | Grants the permission to view discounts                                                                                                    | read         | -                           | -             | -     |
| billing:balance:view          | Grants the permission to view income and expense details, historical payment records, consumption quotas, adjustment records, and arrears. | list         | -                           | -             | -     |
| billing:coupon:view           | Grants the permission to view coupons, stored value cards, and cash coupons.                                                               | read         | -                           | -             | -     |
| billing:order:view            | Grants the permission to view order information and pay-per-use packages.                                                                  | list         | -                           | -             | -     |
| billing:order:pay             | Grants the permission to pay orders.                                                                                                       | write        | -                           | -             | -     |
| billing:subscription:view     | Grants the permission to view renewals and query resources that can be changed from pay-per-use to yearly/monthly.                         | read         | -                           | -             | -     |

| Action                               | Description                                                                                                                                         | Access Level | Resource Type (*: required) | Condition Key | Alias |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| billing:subscription:renew           | Grants the permission to renew subscriptions, enable auto-renewal, set expiration policies, and change pay-per-use subscriptions to yearly/monthly. | write        | -                           | -             | -     |
| billing:subscription:unsubscribe     | Grants the permission to view unsubscribed resources, unsubscribe from resources, cancel delivery, and return or replace hardware.                  | write        | -                           | -             | -     |
| billing:resourcePackages:view        | Grants the permission to view resource packages and remaining amount and query or export usage details.                                             | list         | -                           | -             | -     |
| billing:billDetail:view              | Grants the permission to view order details.                                                                                                        | read         | -                           | -             | -     |
| billing:bill:view                    | Grants the permission to view bills, expenditures of the current month, paid resources in the last seven days, and expenditure trends.              | list         | -                           | -             | -     |
| costCenter:costAnalysis:listCosts    | Grants the permission to view cost analysis.                                                                                                        | read         | -                           | -             | -     |
| Billing::activeEP Finance            | Grants the permission to enable the enterprise project function.                                                                                    | write        | -                           | -             | -     |
| businessUnitCenter:businessUnit:view | Grants the permission to view organizations and accounts.                                                                                           | read         | -                           | -             | -     |

| Action                 | Description                                                                                          | Access Level | Resource Type (*: required) | Condition Key | Alias |
|------------------------|------------------------------------------------------------------------------------------------------|--------------|-----------------------------|---------------|-------|
| billing:invoice:manage | Grants the permission to manage invoices, request invoices, and manage invoice titles and addresses. | write        | -                           | -             | -     |

Each API usually supports one or more actions. [Table 3-313](#) lists the supported actions and dependencies.

#### NOTE

If fine-grained authentication fails, the value of **encoded\_authorization\_message** in the response can be viewed only after being decrypted by calling the API provided by STS. APIE address of the decryption API: [Decoding the Authentication Failure Cause](#).

Note: The caller must have the **sts::decodeAuthorizationMessage** permission to call the decryption API on APIE. Otherwise, the error message "STS5.1001" is displayed.

**Table 3-313** Actions and dependencies supported by BSS APIs

| Scenario          | Sub-Scenario                          | API                                   | API URL                                                | Action                        | Action                                 | Dependency |
|-------------------|---------------------------------------|---------------------------------------|--------------------------------------------------------|-------------------------------|----------------------------------------|------------|
| Managing products | Querying product price                | Querying pay-per-use product price    | POST /v2/bills/ratings/on-demand-resources             | billing:contract:viewDiscount | Viewing discount and price information | -          |
|                   | Querying yearly/monthly product price | Querying yearly/monthly product price | POST /v2/bills/ratings/period-resources/subscribe-rate | billing:contract:viewDiscount | View discount and price information.   | -          |

| Scenario          | Sub-Scenario           | API                                                            | API URL                                                  | Action                        | Action                                 | Dependency |
|-------------------|------------------------|----------------------------------------------------------------|----------------------------------------------------------|-------------------------------|----------------------------------------|------------|
|                   |                        | Querying the renewal amount of yearly/monthly resources        | POST /v2/bills/ratings/period-resources/renew-rate       | billing:contract:viewDiscount | Viewing discount and price information | -          |
| Managing products | Querying product price | Querying yearly/monthly resource refunds before unsubscription | POST /v2/bills/ratings/period-resources/unsubscribe-rate | billing:contract:viewDiscount | Viewing discount and price information | -          |
| Managing accounts | Managing accounts      | Querying account balance                                       | GET /v2/accounts/customer-accounts/balances              | billing:balance:view          | View account information.              | -          |

| Scenario              | Sub-Scenario                   | API                          | API URL                                              | Action                        | Action                                                                                                                                     | Dependency |
|-----------------------|--------------------------------|------------------------------|------------------------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|------------|
|                       |                                | Querying consumption quota   | GET /v2/accounts/customer-accounts/expenditure-quota | billing:balance:view          | Grants the permission to view income and expense details, historical payment records, consumption quotas, adjustment records, and arrears. | -          |
| Managing transactions | Managing coupons               | Listing coupons              | GET /v2/promotions/benefits/coupons                  | billing:coupon:view           | View discount, cash, and flexi-purchase coupons.                                                                                           | -          |
|                       | Managing yearly/monthly orders | Listing orders               | GET /v2/orders/customer-orders                       | billing:order:view            | View order information.                                                                                                                    | -          |
|                       |                                | Querying order details       | GET /v2/orders/customer-orders/details/{order_id}    | billing:order:view            | View order information.                                                                                                                    | -          |
|                       |                                | Querying available discounts | GET /v2/orders/customer-orders/order-discounts       | billing:contract:viewDiscount | Viewing discount and price information                                                                                                     | -          |
|                       |                                | Paying yearly/monthly orders | POST /v3/orders/customer-orders/pay                  | billing:order:pay             | Pay orders.                                                                                                                                | -          |

| Scenario | Sub-Scenario                      | API                                                | API URL                                             | Action                                                                                                                                     | Action                                                                                                                                                      | Dependency |
|----------|-----------------------------------|----------------------------------------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|          |                                   | Querying refund order amount                       | GET /v2/orders/customer-orders/refund-orders        | billing:order:view                                                                                                                         | View order information.                                                                                                                                     | -          |
|          | Managing yearly/monthly resources | Listing yearly/monthly resources                   | POST /v2/orders/subscriptions/resources/query       | <ul style="list-style-type: none"> <li>• billing:subscription:view</li> <li>• billing:order:view <b>(to be brought offline)</b></li> </ul> | View order information.                                                                                                                                     | -          |
|          |                                   | Renewing subscriptions to yearly/monthly resources | POST /v2/orders/subscriptions/resources/renew       | billing:subscription:renew                                                                                                                 | Place orders, cancel orders, and modify recipient information.                                                                                              | -          |
|          |                                   | Unsubscribing from yearly/monthly resources        | POST /v2/orders/subscriptions/resources/unsubscribe | billing:subscription:unsubscribe                                                                                                           | Place orders, cancel orders, and modify recipient information.<br>For details, see <a href="#">FAQs About Cloud Service Unsubscription Authentication</a> . | -          |

| Scenario | Sub-Scenario | API                                                                              | API URL                                                           | Action                     | Action                                                         | Dependency |
|----------|--------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------|----------------------------------------------------------------|------------|
|          |              | Enabling automatic renewal for yearly/monthly resources                          | POST /v2/orders/subscriptions/resources/autorenew/**              | billing:subscription:renew | Place orders, cancel orders, and modify recipient information. | -          |
|          |              | Disabling automatic renewal for yearly/monthly resources                         | DELETE /v2/orders/subscriptions/resources/autorenew/{resource_id} | billing:subscription:renew | Place orders, cancel orders, and modify recipient information. | -          |
|          |              | Enabling/Canceling the change from yearly/monthly to pay-per-use upon expiration | POST /v2/orders/subscriptions/resources/to-on-demand              | billing:subscription:renew | Place orders, cancel orders, and modify recipient information. | -          |



| Scenario | Sub-Scenario               | API                                                                                                                    | API URL                                              | Action                        | Action                                                                                                 | Dependency |
|----------|----------------------------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------|------------|
|          |                            | Setting a deduction date for auto-renewal of yearly/monthly resources and a same expiration date for renewed resources | POST /v2/orders/subscriptions/resources/renew/config | billing:subscription:renew    | Place orders, cancel orders, and modify recipient information.                                         | -          |
|          | Managing resource packages | Listing resource packages                                                                                              | POST /v3/payments/free-resources/query               | billing:resourcePackages:view | View bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends. | -          |

| Scenario       | Sub-Scenario   | API                                     | API URL                                                   | Action                                                                                                                                          | Action                                                                                                 | Dependency |
|----------------|----------------|-----------------------------------------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------|
|                |                | Querying resource package usage details | GET /v2/bills/customer-bills/free-resources-usage-records | <ul style="list-style-type: none"> <li>billing:resourcePackages:view</li> <li>billing:billDetail:view <b>(to be brought offline)</b></li> </ul> | View expenditure details, resource expenditures, bill analysis, and historical payments.               | -          |
|                |                | Querying resource package usage         | POST /v2/payments/free-resources/usages/details/query     | billing:resourcePackages:view                                                                                                                   | View bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends. | -          |
| Managing bills | Managing bills | Viewing bill details                    | POST /v2/bills/customer-bills/res-records/query           | billing:billDetail:view                                                                                                                         | View expenditure details, resource expenditures, bill analysis, and historical payments.               | -          |

| Scenario       | Sub-Scenario   | API                                    | API URL                                      | Action                                                                                                                               | Action                                                                                                 | Dependency |
|----------------|----------------|----------------------------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------|
|                |                | Querying bill summary                  | GET /v2/bills/customer-bills/monthly-sum     | billing:bill:view                                                                                                                    | View bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends. | -          |
|                |                | Querying expenditure records           | GET /v2/bills/customer-bills/res-fee-records | <ul style="list-style-type: none"><li>• billing:billDetail:view</li><li>• billing:bill:view <b>(to be brought offline)</b></li></ul> | View bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends. | -          |
| Managing bills | Managing bills | Querying expenditure records for iQIYI | GET /v2/bills/customer-bills/res-fee-details | billing:bill:view                                                                                                                    | View bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends. | -          |

| Scenario            | Sub-Scenario                 | API                                                       | API URL                                                         | Action                            | Action                                                                                                 | Dependency |
|---------------------|------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------|--------------------------------------------------------------------------------------------------------|------------|
|                     |                              | Querying bill details of a device resource                | GET /v2/bills/customer-bills/res-merge-records                  | billing:billDetail:view           | View expenditure details, resource expenditures, bill analysis, and historical payments.               | -          |
|                     |                              | Querying expenditure summary of customer resources by day | POST /v1.0/{domain_id}/customer/account-mgr/bill/resource-daily | billing:bill:view                 | View bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends. | -          |
| Managing costs      | Managing costs               | Querying cost data                                        | POST /v4/costs/cost-analysed-bills/query                        | costCenter:costAnalysis:listCosts | View cost analysis.                                                                                    | -          |
| Managing enterprise | Managing enterprise projects | Enabling the enterprise project management service        | POST /v2/enterprises/enterprise-projects/authority              | Billing::activateEPFinance        | Enable the enterprise project management service.                                                      |            |

| Scenario                     | Sub-Scenario                        | API                                            | API URL                                                                    | Action                               | Action                                                    | Dependency |
|------------------------------|-------------------------------------|------------------------------------------------|----------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------------|------------|
|                              | Managing enterprise member accounts | Querying enterprise member accounts            | GET /v2/enterprises/multi-accounts/sub-customers                           | businessUnitCenter:businessUnit:view | View organizations and accounts in the Enterprise Center. | -          |
| Managing costs               | Managing costs                      | Querying cost analysis results                 | POST /v3/costs/cost-analysed-bills/query                                   | costCenter:costAnalysis:listCosts    | View cost analysis.                                       | -          |
|                              |                                     | Querying cost analysis results                 | POST /v2/costs/cost-analysed-bills/query                                   | costCenter:costAnalysis:listCosts    | View cost analysis.                                       | -          |
| Managing enterprise accounts | Managing enterprise accounts        | Changing the fund quota of enterprise projects | PUT /v1.0/{domain_id}/customer/enterprise-project/fund-quotas              | Billing::updateEPFundQuota           | Change the enterprise project fund quota.                 | -          |
|                              |                                     | Querying enterprise project fund quotas        | POST /v1.0/{domain_id}/customer/enterprise-project/fund-quotas/batch-query | Billing::viewEPFundQuota             | Query the enterprise project fund quota.                  | -          |

| Scenario          | Sub-Scenario      | API                                         | API URL                                                          | Action                       | Action                                         | Dependency |
|-------------------|-------------------|---------------------------------------------|------------------------------------------------------------------|------------------------------|------------------------------------------------|------------|
|                   |                   | Disabling the enterprise project fund quota | DELETE /v1.0/{domain_id}/customer/enterprise-project/fund-quotas | Billing::activateEPFundQuota | Change the enterprise project fund quota.      | -          |
|                   |                   | Enabling the enterprise project fund quota  | POST /v1.0/{domain_id}/customer/enterprise-project/fund-quotas   | Billing::activateEPFundQuota | Change the enterprise project fund quota.      | -          |
| Managing invoices | Managing invoices | Listing invoices                            | GET /v1.0/{domain_id}/payments/intl-invoices                     | billing:invoice:manage       | Request invoices and view invoice information. | -          |

## Resources

BSS does not support resource-specific permission control in identity policies. If you want to allow access to BSS, use the wildcard (\*) for the Resource element to apply policies to all resources.

## Conditions

A Condition element lets you specify conditions for when an identity policy is in effect. It contains [condition keys](#) and [operators](#).

- The condition key that you specify can be a global condition key or a service-specific condition key.
  - Global condition keys (with the **g:** prefix) apply to all actions. Cloud services do not need to provide user identity information. Instead, the system automatically obtains such information and authenticates users. For details, see [Global Condition Keys](#).
  - Service-specific condition keys (with the abbreviation of a service name plus a colon as the prefix, for example, **BSS:**) only apply to operations of the BSS service. For details, see [Table 3-314](#).

- The number of values associated with a condition key in the request context of an API call makes the condition key single-valued or multivalued. Single-valued condition keys have at most one value in the request context of an API call. Multivalued condition keys can have multiple values in the request context of an API call. For example, a request can originate from at most one VPC endpoint, so `g:SourceVpce` is a single-valued condition key. You can tag resources and include multiple tag key-value pairs in a request, so `g:TagKeys` is a multivalued condition key.
- A condition operator, condition key, and a condition value together constitute a complete condition statement. An identity policy can be applied only when its request conditions are met. For supported condition operators, see .

The following table lists the condition keys that you can define in identity policies for BSS. You can include these condition keys to specify conditions for when your identity policy is in effect.

**Table 3-314** Service-specific condition keys supported by BSS

| Service-specific Condition Key | Type   | Single-valued/<br>Multivalued | Description                                                                                               |
|--------------------------------|--------|-------------------------------|-----------------------------------------------------------------------------------------------------------|
| billing:cloudServiceType       | string | Multi-value                   | Filter access based on the cloud service type specified in the request parameter.<br><a href="#">FAQs</a> |

### Condition Key Examples

- billing:cloudServiceType

Example: Only orders of cloud service resources whose service type is **hws.service.type.ebs** can be unsubscribed from.

```
{
  "Version": "5.0",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "billing:subscription:unsubscribe"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "billing:cloudServiceType": [
          "hws.service.type.ebs"
        ]
      }
    }
  ]
}
```