Organizations

User Guide

Issue	01
Date	2025-02-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Contents

1 Permissions Management

1.1 Creating an IAM User and Granting Organizations Permissions

This section describes how a management account creates an IAM user and grants organization administrator permissions to the user.

You can use Identity and Access Management (IAM) for fine-grained permissions control on Organizations. With IAM, you can:

- Grant users only the permissions required to perform a given task based on their job responsibilities. For example, you use the management account to create two IAM users, and assign one of them the permissions to create and delete OUs while the other one only the permission to view information about OUs.
- Use the management account to create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials to access Huawei Cloud and use Organizations, improving account security.
- Entrust another Huawei Cloud account or a cloud service to perform efficient O&M on your Organizations.

If your HUAWEI ID or Huawei Cloud cloud account meets your permissions requirements, you can skip this section.

The following describes how to create an IAM user and grant permissions to the user. **Figure 1-1** illustrates an example process.

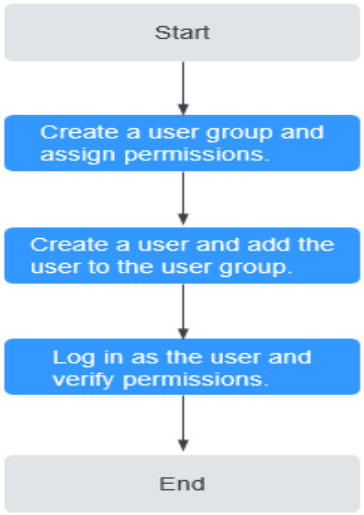
Prerequisites

Before assigning permissions to user groups, learn about the permissions supported by Organizations, as described in Permissions.

For the permissions of other services, see System Permissions.

Process Flow

Figure 1-1 Process of granting Organizations permissions



1. On the IAM console, Create a user group and assign permissions (**OrganizationsReadOnlyAccess** as an example).

   Create a user group on the IAM console to assign the **Organizations ReadOnlyAccess** permissions to the group.
2. Create an IAM user and add it to the user group.

   Create a user on the IAM console and add it to the user group created in **1**.
3. Log in and verify permissions.

   Log in to the console as the IAM user. If you can access Organizations and view organization information but encounter an error message when you attempt to add an OU, saying "Insufficient permission. Contact the administrator", the **Organizations ReadOnlyAccess** policy has been applied and you have only the permission to view organization information.

1.2 Creating Custom Policies

You can create custom policies to supplement the system-defined policies of Organizations. For the actions that can be added to custom policies, see Policies and Supported Actions.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. There is no need to know much about policy syntax.
- JSON: Edit policies from scratch or based on an existing policy in JSON format.

For details, see Creating a Custom Policy. The following lists examples of common Organizations custom policies.

Example Custom Policies

- Example 1: Grant permission to invite member accounts to join an organization or to remove member accounts from an organization.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:accounts:invite",
                "organizations:accounts:remove"
            ]
        }
    ]
}
```

- Example 2: Grant permission to deny the deletion of OUs or removal of member accounts.

  To apply a policy with only Deny statements, it must be used together with other policies. If you do not assign the permission to perform an action, the action is denied by default. If the permissions granted to an IAM user contain both Allow and Deny, **the Deny statements take precedence over the Allow statements**.

  Assume that you want to grant the permissions of the **OrganizationsFullAccess** policy to a user but want to prevent them from deleting OUs or removing member accounts. You can create a custom policy for denying the deletion, and attach this policy together with the **OrganizationsFullAccess** policy to the user. As an explicit Deny in any policy overrides any kind of Allow, the user can perform all operations on a given organization except deleting its OUs or removing member accounts. The following is an example of a deny policy:

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "organizations:ous:delete",
                "organizations:accounts:remove"
            ]
        }
    ]
}
```


2 Managing Organizations

2.1 Overview of Organizations

What Is Organizations?

An organization is an entity that you create to manage multiple accounts. Each organization is composed of exactly one management account, multiple member accounts, and one root with many OUs organized in a hierarchical, tree-like structure. You can group member accounts into the root or any of the OUs. For details about the basic concepts of Organizations, see Basic Concepts.

Helpful links:

- **Creating an Organization**: You can use your current account as the management account to create an organization and invite other accounts to join your organization.
- **Viewing Details About an Organization**: You can view details about your organization, root, OUs, and accounts.
- **Deleting an Organization**: You can delete an organization when you no longer need it.

2.2 Creating an Organization

You can use a Huawei Cloud account as the management account to create an organization. After creating the organization, you can **invite existing accounts** or **create new accounts** to add them to your organization, and you can **create OUs** to manage accounts in your organization.

Prerequisites

The current account has not joined any organization. If this account is already in an organization and you still need to use it, remove it from the current organization and then use it to create your organization. For how to remove from an organization, see **Leaving an Organization As a Member Account**.

The current account must have enabled Enterprise Center and become an enterprise master account. For details, see Enabling Enterprise Center.

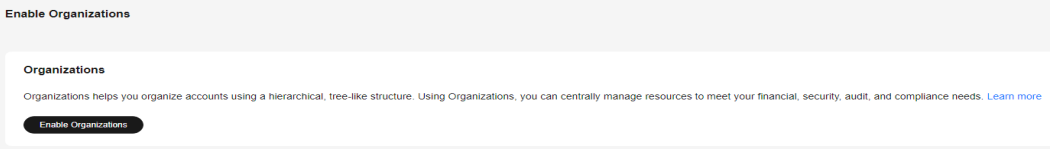
Procedure

You can create an organization on the management console or by calling Organizations APIs. The following describes how to create an organization on the console.

Step 1 Log in to Huawei Cloud, and navigate to the Organizations console.

Step 2 Click **Enable Organizations** to enable the Organizations service.

Figure 2-1 Enabling Organizations



After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account.

----End

Then, you can **invite existing accounts to join your organization** or **create new accounts in your organization**, and you can also **create OUs** to manage accounts.

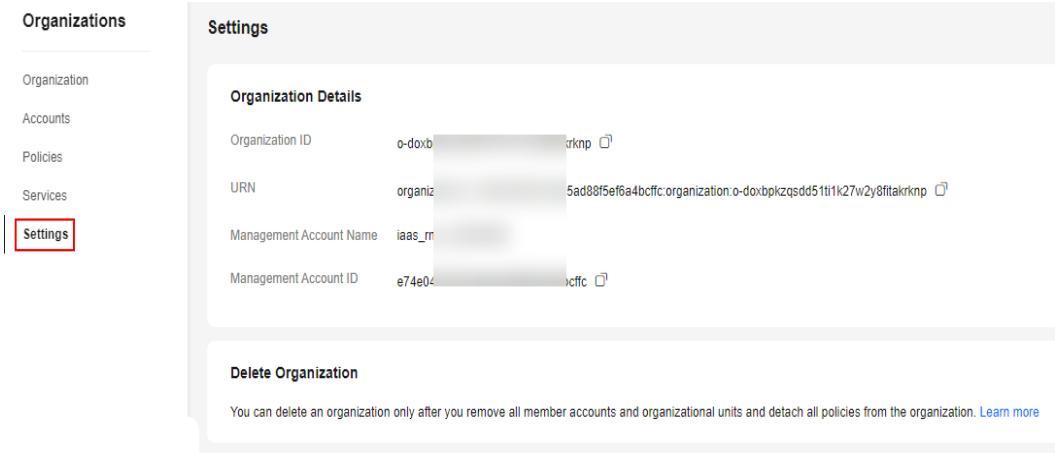
2.3 Viewing Details About an Organization

You can use the management account to view all information about your organization. The member accounts can view only the organization ID, management account name, and management account ID.

Viewing Organization Details from the Management Account

Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Settings** page to view information such as the organization ID, URN, management account name, and management account ID.

Figure 2-2 Viewing organization details from the management account



Viewing Root Details from the Management Account

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Click the organization root. You can view details about the root on the right of the organization tree, including the root ID, time of creation, URN, policies, and tags.

----End

Viewing OU Details from the Management Account

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Click the OU. You can view details about the OU on the right of the organization tree, including the OU name, ID, URN, when the OU was created, as well as policies and tags attached.

----End

Viewing Account Details from the Management Account

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Click the account. You can view details about the selected account on the right of the organization tree, including the account name, account ID, URN, time when the account joined the organization, parent OU, as well as policies, tags, and agency services associated with the account.

----End

Viewing Organization Details from a Member Account

Log in to Huawei Cloud as a member account, navigate to the Organizations console, and access the **Settings** page to view the organization ID, URN, management account name, and management account ID.

2.4 Deleting an Organization

Prerequisites

You can delete an organization when you no longer need it.

NOTE

An organization can be deleted only after all member accounts, OUs, and policies are removed from the organization.

Impacts

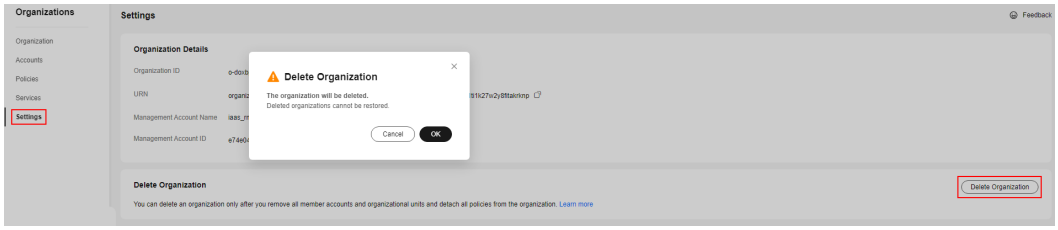
- **Impacts on the Management Account**
  - The management account will become a standalone account. You can use it to create a different organization or accept an invitation from another organization to add the account to that organization as a member account.
  - The management account of an organization is never affected by service control policies (SCPs). There is no change to the permissions assigned to the management account and its IAM users.
- **Impact on Member Accounts**
  - Each member account will become a standalone account. You can use it to create a different organization or accept an invitation from another organization to add the account to that organization as a member account.
  - After the organization is deleted, member accounts are no longer affected by SCPs, and the permissions assigned to the member accounts and their IAM users may change.
- **Impact on Policies**
  - If you delete an organization, you cannot recover it. If you have created SCPs inside the organization, they are also deleted and you cannot recover them.

Procedure

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Settings** page.

Step 2 Click **Delete Organization**. In the displayed dialog box, click **OK**.

Figure 2-3 Deleting an organization



----End

3 Managing OUs

3.1 Overview of an OU

What Is an OU?

An organizational unit (OU) is a container or a logical grouping of accounts in your organization. You can use OUs to group accounts together to administer them as a single unit. An OU can be mapped to a department, a subsidiary, or a project team. You can create OUs within other OUs. Each OU can have only one parent OU, but they can have many other child OUs or member accounts.

Helpful links:

- **Creating an OU**
- **Modifying an OU**
- **Viewing Details About an OU**
- **Deleting an OU**

3.2 Creating an OU

You can create an OU in your organization's root. OUs can be nested up to five levels deep.

To create an OU:

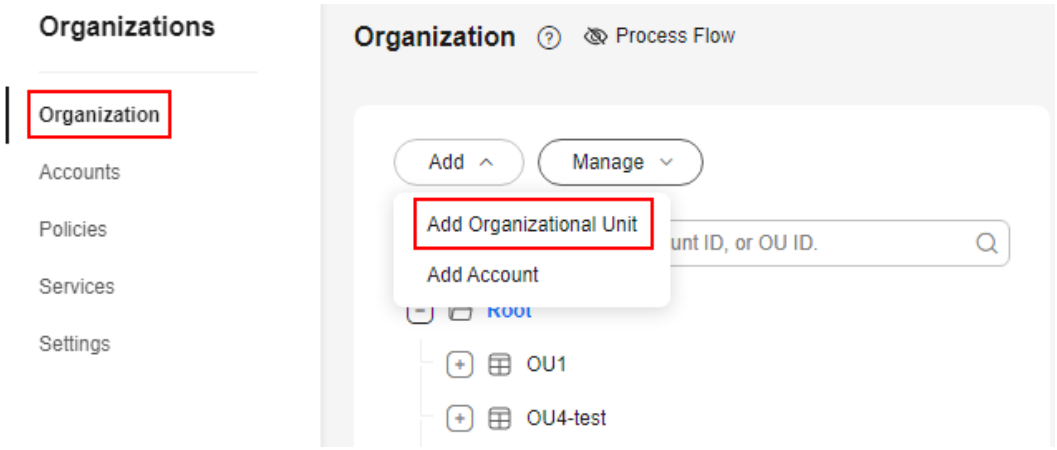
Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the parent OU by clicking its name rather than the expand icon. If you are creating an OU for the first name, select the **Root** OU.

OUs can be nested up to five levels deep. Each OU can have only one parent OU but can have many child OUs. When creating an OU, ensure that the parent OU you select is the upper-level one.

Step 3 Choose **Add** > **Add Organizational Unit**.

Figure 3-1 Adding an OU



Step 4 In the displayed dialog box, enter the OU name.

Step 5 (Optional) Add a tag to the OU.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for OUs. A maximum of 20 tags can be added to an OU.

Table 3-1 describes the key and value descriptions of a tag.

Table 3-1 Tag description

Element	Description	Example
Tag key	A tag key of an OU must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS). A tag key: • Cannot be an empty string. • Contains 1 to 128 characters. • Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF).	Key_0001
Tag value	A tag value can be repetitive or an empty string. A tag value: • Can be an empty string. • Contains 1 to 225 characters. • Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF).	Value_0001

Step 6 Click **OK**.

----End

3.3 Modifying an OU

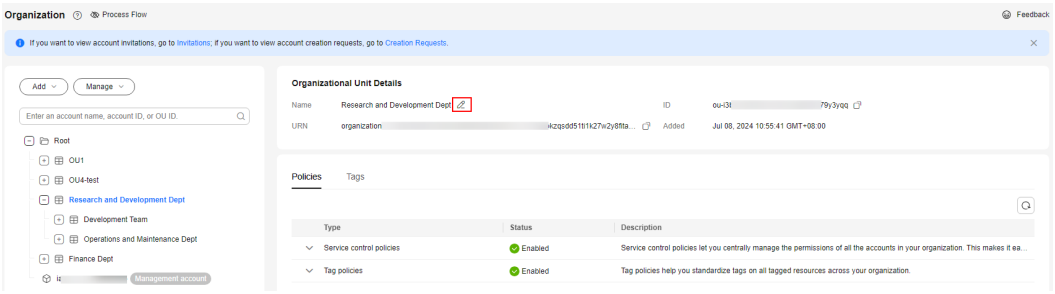
After an OU is created, you can modify its name, tag, and policy at any time. For details about how to modify tags and policies, see **Managing Tags** and **Attaching or Detaching an SCP**.

Procedure

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU you want to rename and click next to the OU name on the displayed OU details page.

Figure 3-2 Renaming an OU



Step 3 Enter a new name for the OU and click to save it.

----End

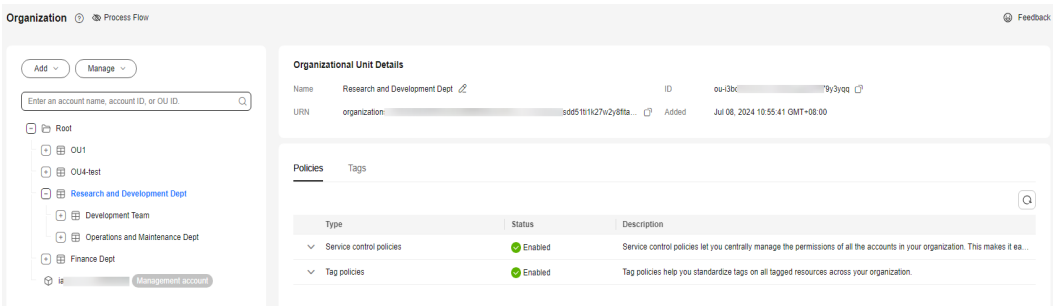
3.4 Viewing Details About an OU

After an OU is created, you can view its details any time by following the steps below.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Click the OU you want to view. Its details are displayed on the right of the OU tree, including the OU name, ID, URN, time of creation, policies, and tags.

Figure 3-3 Viewing details about an OU



----End

3.5 Deleting an OU

You can delete an OU that is no longer needed.

NOTE

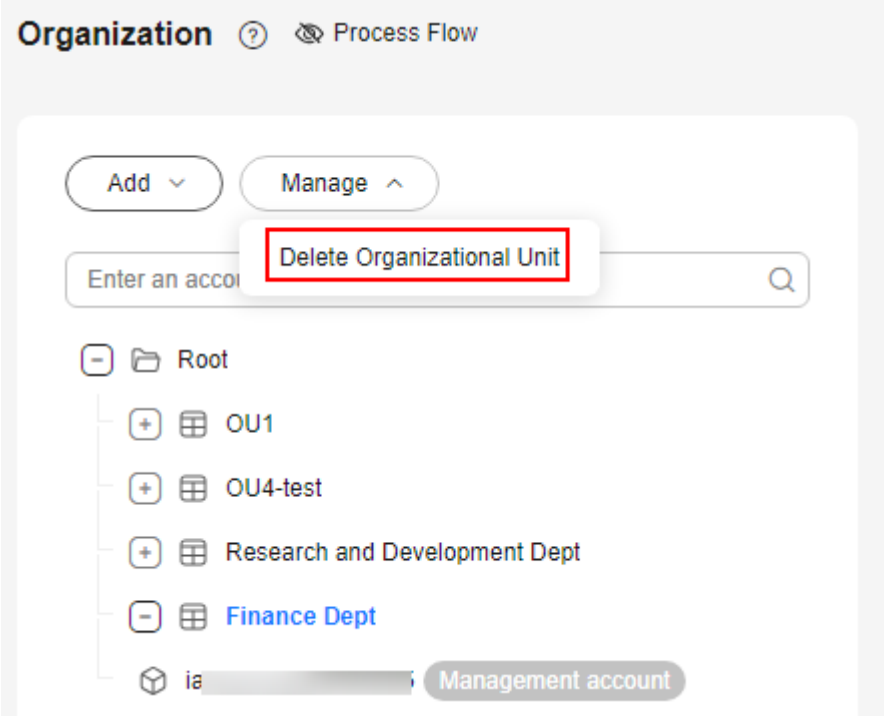
You cannot delete an OU if it contains other OUs or accounts.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Click the OU you want to delete and click **Manage** above the OU tree.

Step 3 Choose **Delete Organizational Unit**. In the displayed dialog box, click **OK**.

Figure 3-4 Deleting an OU



----End

4 Managing Accounts

4.1 Overview of an Account

Accounts in Your Organization

An account is used to contain your Huawei Cloud resources. It is the smallest unit of an organization. Each organization has one management account and multiple member accounts.

Table 4-1 Account types

Account Type	Function	Quota
Management account	With the Organizations service, you can use the management account to create an organization and manage OUs, accounts, and policies for the organization.	1 (Each organization can have exactly one management account.)
Member account	Except for the management account, other accounts in an organization are member accounts. Each member account is part of only one organization at a time. Generally, member accounts hold resources for a specific application or project of an organization.	9

Impacts of Being in an Organization

When you **invite an existing account to your organization** or **create a new account in your organization**, Organizations will automatically make the following changes to the new member account:

- A service-linked agency is created in the member account. It is a cloud service agency with the system-defined permission **OrganizationsServiceLinkedAgencyPolicy** for all resources.

- The permissions of the new member account are affected by service control policies and tag policies. You may have service control policies and tag policies attached to the root or the OU that contains the new member account. If so, the policies will apply to the new member account and all IAM users in the member account.
- When you use the management account to enable a trusted service, the trusted service can create a service-linked agency for that trusted service in the member account.

Helpful links:

- **Inviting an Account to Join Your Organization**: You can create invitations, manage invitations you have sent, and accept or reject invitations.
- **Creating an Account**: You can use the management account to create new accounts.
- **Closing an Account**: You can use the management account to close any unwanted accounts that you have created. Invited accounts cannot be closed.
- **Moving an Account**: You can move accounts from one OU to another OU.
- **Viewing Account Details**: You can view the account name, account ID, the time when it joined an organization, any account-owing OUs, and the policies, tags, and delegated services that are attached to the account.
- **Removing a Member Account from Your Organization**: You can use the management account to remove member accounts from your organization.
- **Viewing Account Records**: When you sign in to the management account of your organization, on the **Accounts** page, you can view account details, including the account list, invitations, and creation requests. You can also invite, create, close, move, remove, and cancel any pending invitations.

4.2 Inviting an Account to Join Your Organization

When you invite a HUAWEI ID or Huawei Cloud account to join your organization, Organizations sends an invitation to the ID or account owner, who then chooses to accept or reject the invitation. You can use the Organizations console to issue and manage invitations that you send to other accounts.

NOTE

The accounts you invite to join your organization must have completed enterprise or individual real-name authentication. For details, see Real-Name Authentication.

The original accounting relationship (master-member association) of invited accounts will remain unchanged.

This section includes the following content:

- **Issuing Invitations to Accounts**
- **Managing Open Invitations of Your Organization**
- **Accepting or Rejecting an Invitation from an Organization**

Issuing Invitations to Accounts

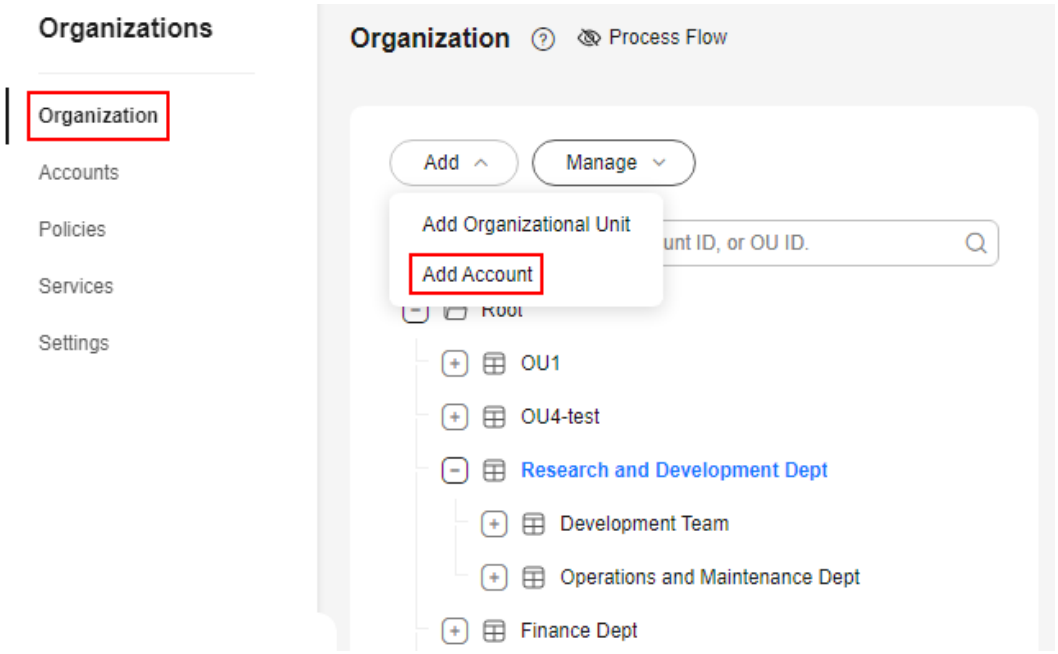
To invite other accounts to join your organization, perform the steps described in this section. By default, those invited accounts will be placed as member accounts

in the root OU. If you want to move them to another OU, see **Moving an Account**.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 On the **Organization** page, choose **Add** > **Add Account**.

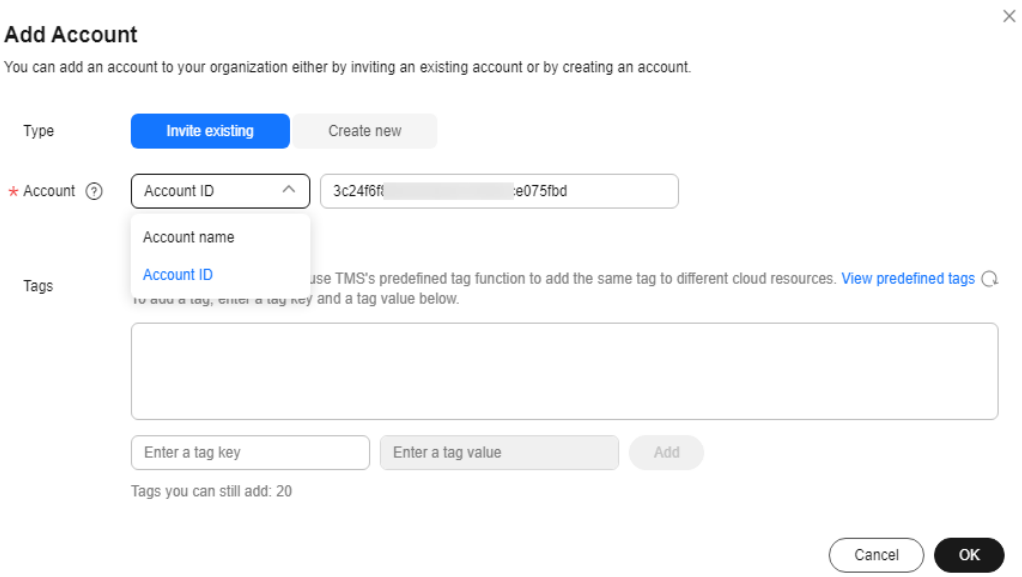
Figure 4-1 Adding an account



Step 3 In the displayed dialog box, select **Invite existing** and enter the name or ID of the account you want to invite.

For details about how to obtain an account name or account ID, see Obtaining Account ID and Name.

Figure 4-2 Inviting an existing account



Step 4 (Optional) Add one or more tags to the account.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for accounts. You can add up to 20 tags to an account.

Table 4-2 describes the key and value descriptions of a tag.

Table 4-2 Tag description

Element	Description	Example
Tag key	A tag key of an account must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS). A tag key: • Cannot be an empty string. • Contains 1 to 128 characters. • Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF).	Key_0001
Tag value	A tag value can be repetitive or an empty string. A tag value: • Can be an empty string. • Contains 1 to 225 characters. • Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF).	Value_0001

Step 5 Click **OK** to send an invitation to the invited account.

----End

Managing Open Invitations of Your Organization

When you log in as the management account, you can view and manage invitations of your organization.

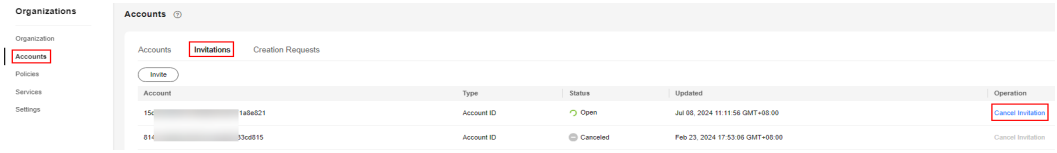
Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Accounts** page.

Step 2 Click the **Invitations** tab. You can view all the invitations sent from your organization and their statuses on the page.

Step 3 Locate the **Open** invitation you want to cancel and click **Cancel Invitation** in the **Operation** column. Then, click **OK** in the displayed dialog box.

After the invitation is canceled, its status changes from **Open** to **Canceled**. If you want that account to join your organization again, you must send a new invitation.

Figure 4-3 Canceling an invitation



----End

Accepting or Rejecting an Invitation from an Organization

Your account may receive an invitation to join an organization. You can accept or reject the invitation.

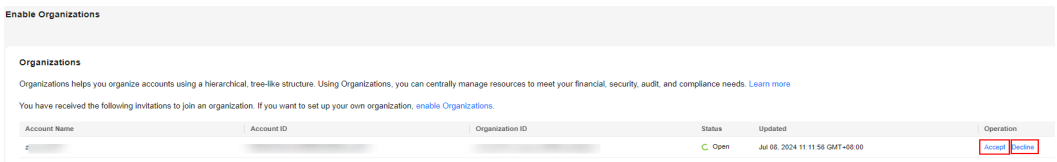
NOTE

Each account can join only one organization. If you receive multiple invitations, you can accept only one of them. If you have joined an organization, you need to exit that organization before accepting an invitation from another organization.

Step 1 Log in to Huawei Cloud as an invited member account, and navigate to the Organizations console.

Step 2 Locate the target invitation and click **Accept** or **Decline** in the **Operation** column. Then, click **OK** in the displayed dialog box.

Figure 4-4 Accepting or rejecting an invitation



----End

4.3 Creating an Account

You can use the management account to create new accounts in your organization. The accounts you created are referred to as resource accounts. For details, see What Are the Differences Between a Resource Account and a Member Account for Unified Accounting? If you want to convert a resource account to a cloud account, refer to Converting a Resource Account to a Cloud Account.

This section includes the following content:

- **Creating an Account**
- **Accessing Account Resources Via Agency**
- **Accessing Account Resources Via IAM Identity Center**

Constraints

- An organization administrator can create a maximum of five accounts at a time.
- The email address associated with the account you are creating cannot be used by another account.
- Accounts created via Organizations can only be used for login only by switching roles via an agency or by accessing the IAM Identity Center console.
- The accounting of accounts created via Organizations is hosted by the organization management account by default.

CAUTION

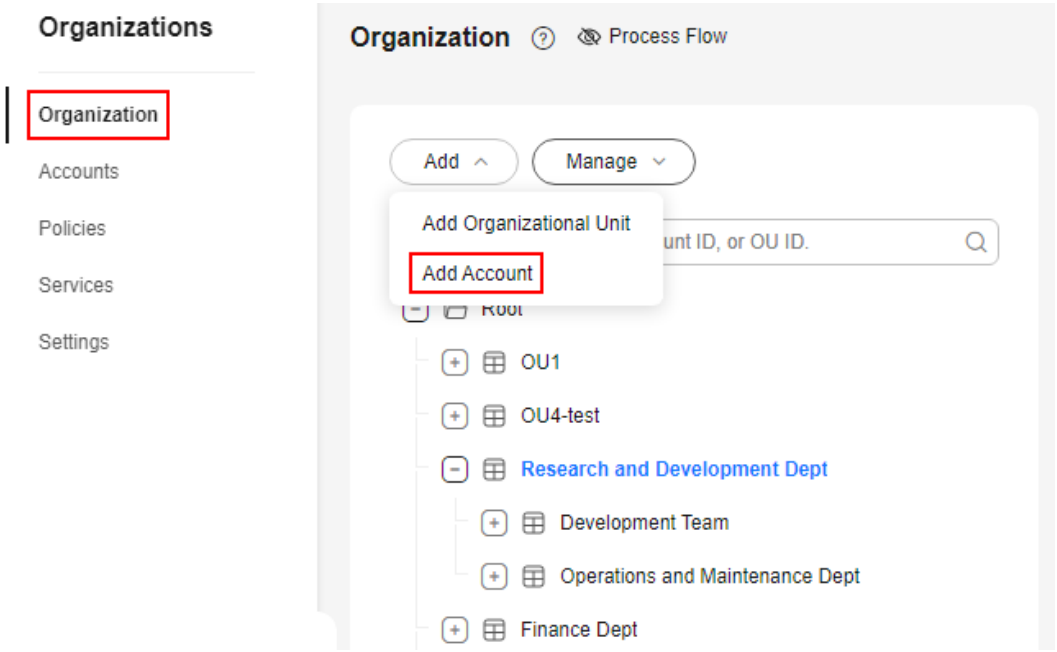
The email address to be associated with the new account must be valid.

Creating an Account

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 On the **Organization** page, choose **Add** > **Add Account**.

Figure 4-5 Adding an account

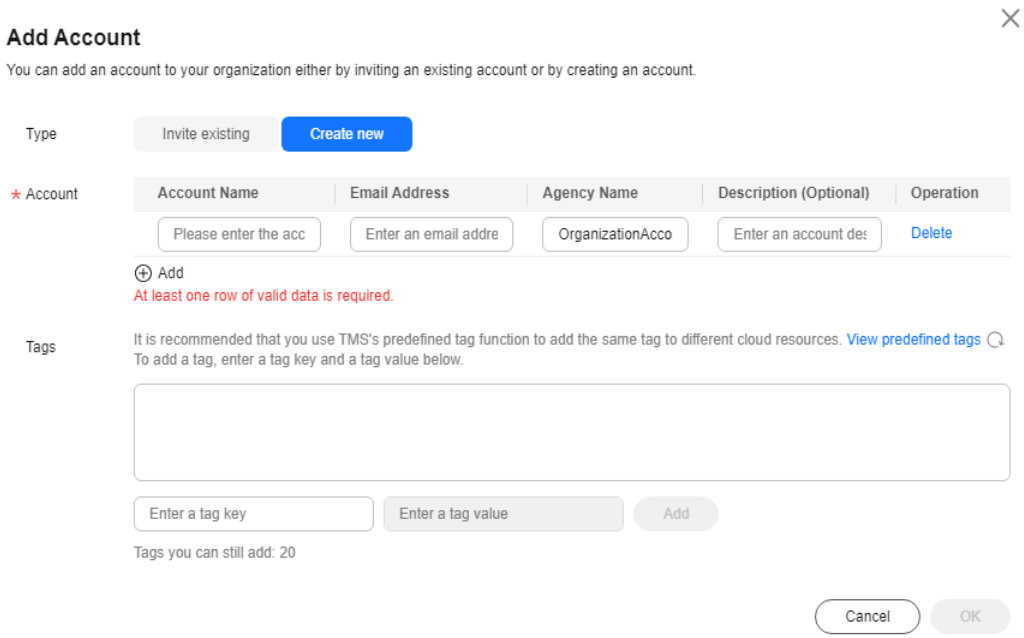


Step 3 Click **Create new** in the displayed dialog box.

Step 4 Enter the account name and email address. Ensure that the account name is different from any existing one.

You can retain the default agency name or change it as required.

Figure 4-6 Creating an account



Step 5 (Optional) Add one or more tags to the account.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for accounts. You can add up to 20 tags to an account.

Table 4-3 describes the key and value descriptions of a tag.

Table 4-3 Tag description

Element	Description	Example
Tag key	A tag key of an account must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS). A tag key: • Cannot be an empty string. • Contains 1 to 128 characters. • Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF).	Key_0001
Tag value	A tag value can be repetitive or an empty string. A tag value: • Can be an empty string. • Contains 1 to 225 characters. • Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF).	Value_0001

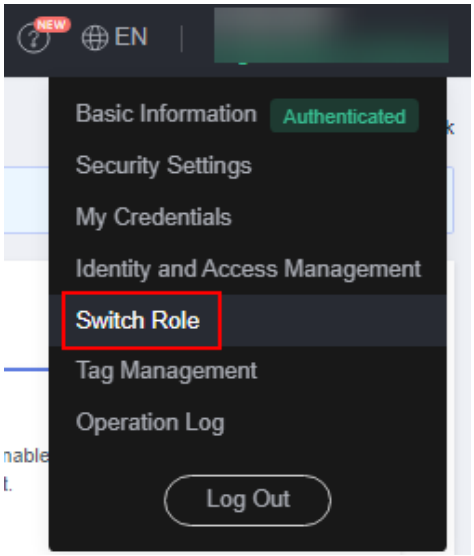
Step 6 Click **OK**. The new account is added to the list.

----End

Accessing Account Resources Via Agency

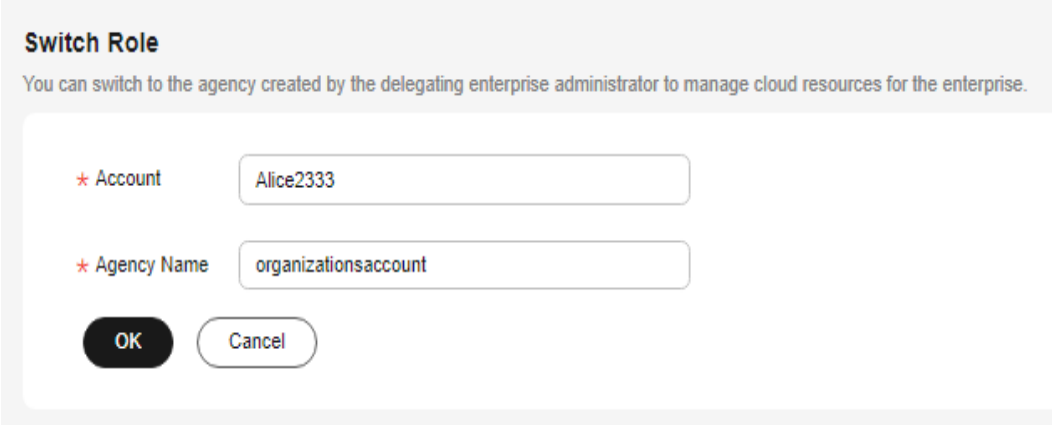
Step 1 Hover the mouse pointer over the username in the upper right corner and choose **Switch Role**.

Figure 4-7 Switching the role



Step 2 On the **Switch Role** page, enter the account name.

Figure 4-8 Entering the account name



NOTE

After you enter the account name, the agencies created under this account will be automatically displayed when you click the agency name text box. An agency name starting with **cbc_** will also be displayed. This agency is mainly used by an enterprise master account to centrally manage expenditures and grant permissions to member accounts. You need to select the agency name entered when creating the account.

Step 3 Click **OK** to switch to the account.

----End

Accessing Account Resources Via IAM Identity Center

You can associate an account with users and permission sets in IAM Identity Center, and log in to the IAM Identity Center console via the user portal URL to access the resources in the account in the given organization. The specific access permission for resources is controlled by the permission set in IAM Identity Center.

Step 1 Associate the account with users and permission sets. For details, see Associating Accounts with Users/Groups and Permission Sets.

Step 2 Log in to the IAM Identity Center console and access the account resources. For details, see Logging In as an IAM Identity Center User and Accessing Resources.

----End

4.4 Closing an Account

If you no longer need a member account, you can close it from the management account of your organization following the instructions in this section. If you want to close the management account, you have to delete your organization. For details, see **Deleting an Organization**.

CAUTION

- Once your request to close an account is submitted, data in the account will start to be deleted and cannot be restored. This operation cannot be undone.
- After the data in an account is deleted, the account status changes to **Closed**. The account will be retained in the account list for 90 days before being permanently deregistered.

Constraints

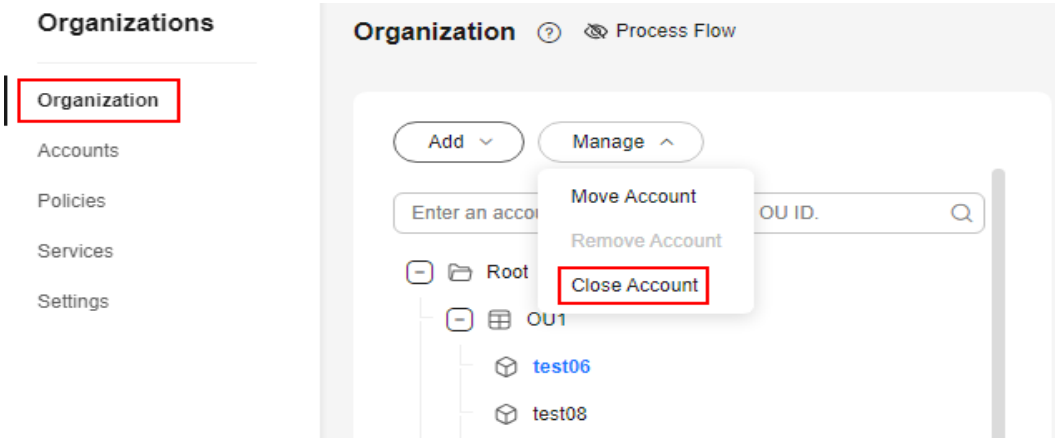
- You can close accounts you created but not those you invited to your organization.
- If any accounts you created have become cloud accounts, they cannot be closed.
- Any account that is specified as a delegated administrator cannot be closed unless you remove the delegated administrator first, as described in **Removing a Delegated Administrator**.
- The management account can only close 10% of the member accounts (no more than 200 accounts) in a given organization within 30 days, and no more than three at a time.
- The mobile number or email address associated with the closing account cannot be used to create another account.
- Any account that has prepaid resources, generally yearly/monthly resources, cannot be closed unless you confirm and unsubscribe from such resources, as described in Unsubscribing from In-Use Resources.
- Any account that has resources in arrears cannot be closed unless you top up your account and pay off the arrears, as described in Top-Up and Payments.

Procedure

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the account you want to close and choose **Manage** > **Close Account**.

Figure 4-9 Closing an account



Step 3 In the displayed dialog box, read and confirm the risks of closing the account, and enter the account name to reconfirm the operation.

Step 4 Click **OK**.

----End

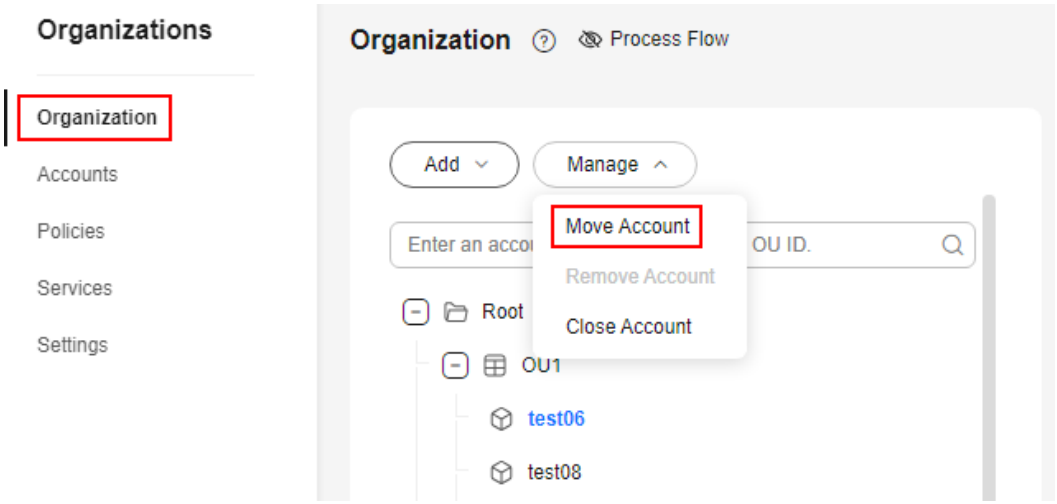
4.5 Moving an Account

When you log in as the management account, you can move an account from one OU to another.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the account you want to move, and choose **Manage** > **Move Account**.

Figure 4-10 Moving an account



Step 3 Select the OU you choose to hold the account, and enter "Confirm" in the text box. Then, click **OK**.

----End

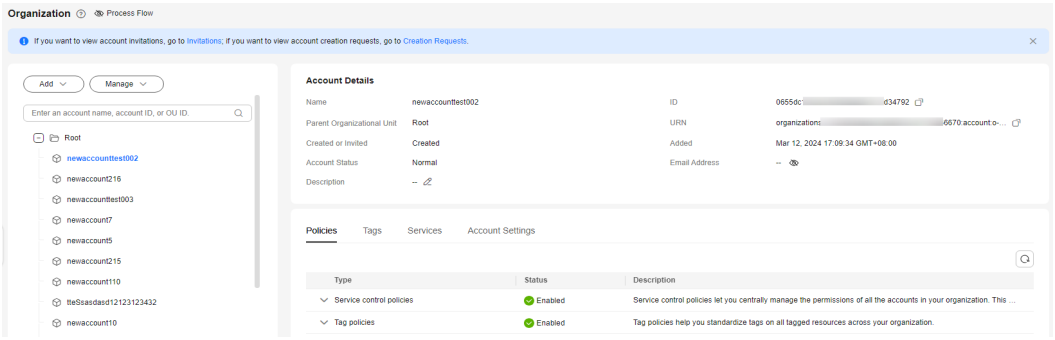
4.6 Viewing Account Details

You can view the details of accounts in your organization at any time by following the steps below.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the account you want to view. Its details are displayed in the pane on the right, including the account name, ID, home OU, URN, how and when the account joined the organization, when the account was created, account status, email address, account description, as well as policies, tags, delegated services.

Figure 4-11 Viewing account details



----End

4.7 Removing a Member Account from Your Organization

Precautions

Before the organization administrator removes a member account from an organization or before a member account leaves an organization, it is important to know the following:

- The member account in question has to have been created more than seven calendar days ago.
- The account has to have been converted to a Huawei Cloud account. For details, see Converting Resource Accounts to Cloud Accounts.
- Invited accounts can be removed from or leave an organization only if they are Huawei Cloud accounts. For details, see Differences Between Resource Accounts and Huawei Cloud Accounts.
- A delegated administrator account cannot be removed from or leave an organization. You need to remove the delegated administrator first. For details, see **Removing a Delegated Administrator**.
- After an account created via Organizations leaves an organization, the IAM agency created by default during the creation of the account will not be automatically deleted. The organization management account can still use that agency to access data of member accounts. To prevent unauthorized access, you need to manually delete the agency. For details, see Deleting or Modifying Agencies.
- After an account created via Organizations leaves the organization, the accounting relationship between the account and the organization management account remains unchanged. After an account that was invited to join an organization leaves the organization, its original accounting relationship remains unchanged. For details about how to disassociate a member account, see Disassociating Member Accounts.
- After a member account leaves an organization, the permissions assigned by the organization policies will no longer apply. This means that the account may actually have more permissions than before. If you enabled trusted access for a cloud service, the account can no longer use the functions of that trusted service.

- When a member account leaves an organization, all tags attached to the account are deleted.

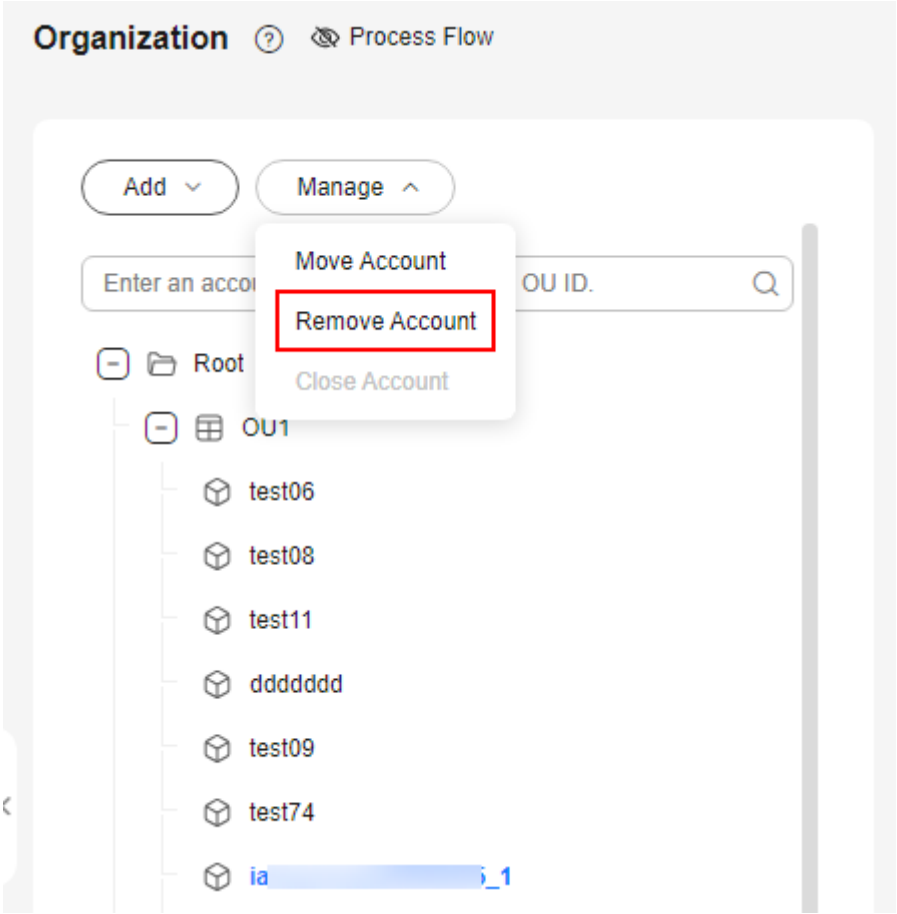
Removing an Account

When you sign in to the management account of your organization, you can remove member accounts that you no longer need. The following steps apply only when you remove member accounts. If you want to remove the management account, you must delete the organization by following the instructions in **Deleting an Organization**.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

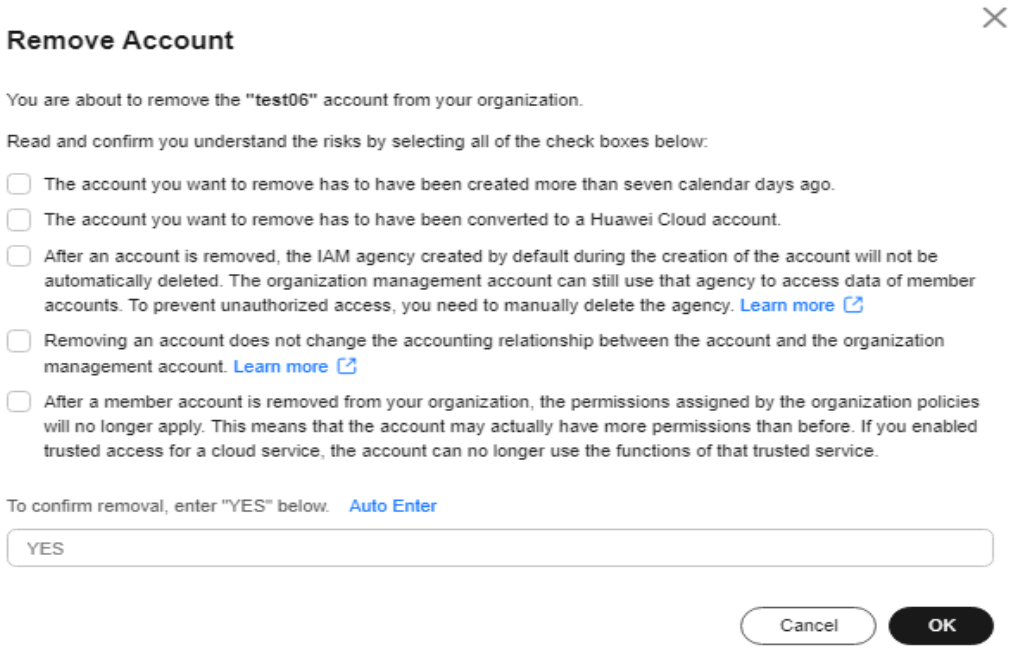
Step 2 Select the account you want to remove, and choose **Manage** > **Remove Account**.

Figure 4-12 Removing an account



Step 3 In the displayed dialog box, read and confirm you understand the risks by selecting all of the check boxes, and then enter **YES** and click **OK**.

Figure 4-13 Confirming the risks of removing the account



----End

Leaving an Organization As a Member Account

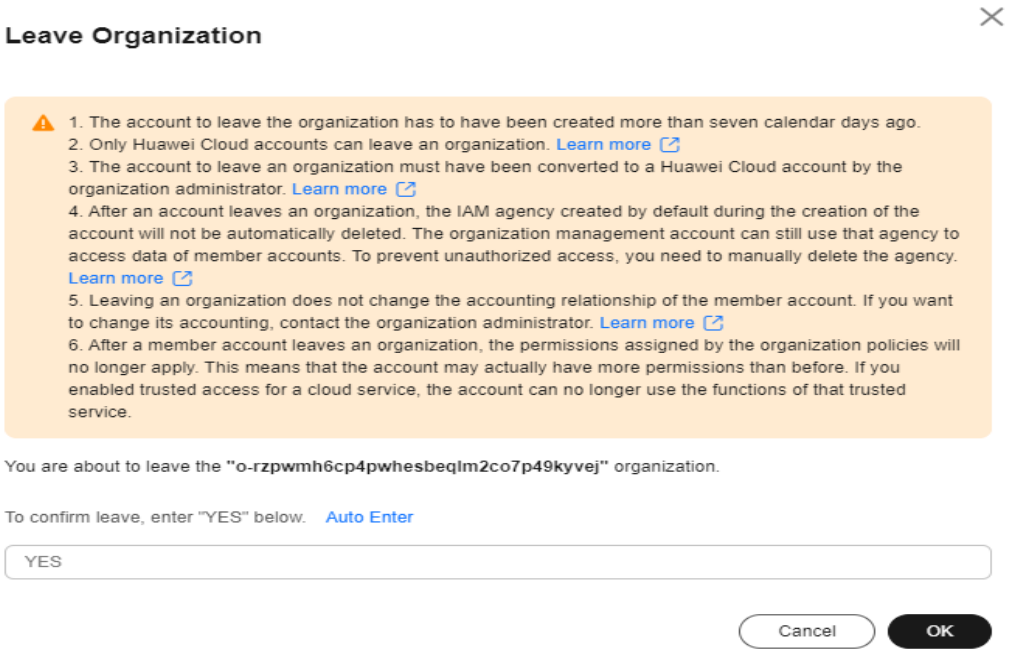
When you sign in to a member account of an organization, you can choose to leave the organization. The management account cannot leave the organization using this method. To remove the management account, you must delete the organization by referring to **Deleting an Organization**.

Any account that is specified as a delegated administrator cannot leave an organization unless you remove the delegated administrator first, as described in **Removing a Delegated Administrator**.

Step 1 Log in to Huawei Cloud as a member account, and navigate to the Organizations console.

Step 2 On the **Settings** page, click **Leave Organization**. In the displayed dialog box, read and confirm you understand the risks, and then enter **YES** and click **OK**.

Figure 4-14 Confirming the risks of leaving the organization



----End

4.8 Viewing Account Records

When you sign in to the management account of your organization, on the **Accounts** page, you can view account details, including the account list, invitations, and creation requests. You can also invite, create, close, move, remove, and cancel any pending invitations.

This section includes the following content:

- **Viewing the Account List**
- **Viewing Invitations**
- **Viewing Creation Requests**

Viewing the Account List

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 Access the **Accounts** page, and click the **Accounts** tab.

In the account list, you can view the details of all the accounts in your organization.

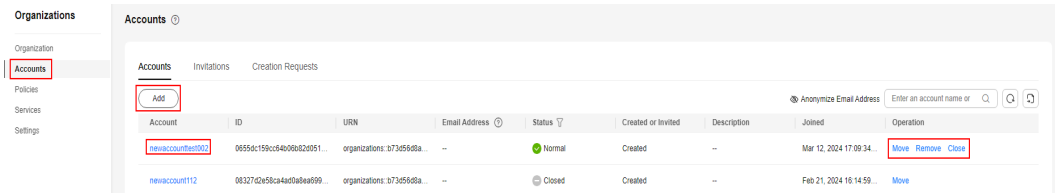
Step 3 Click an account name in the list to view its details.

Step 4 Click **Move** or **Remove**, or **Close** in the **Operation** column.

You cannot close any accounts that have been invited to your organization.

Step 5 Click **Add** in the upper left corner of the list. In the displayed dialog box, you can invite existing accounts to join your organization or create new accounts in the organization.

Figure 4-15 Account list



----End

Viewing Invitations

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

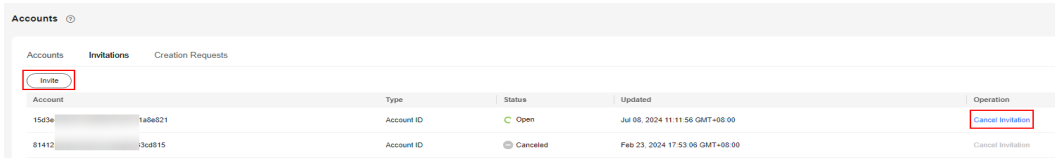
Step 2 On the **Accounts** page, click the **Invitations** tab.

You can view the details about account invitations.

Step 3 Click **Cancel Invitation** in the **Operation** column to cancel an invitation in the **Open** state.

Step 4 Click **Invite** in the upper left corner of the list. In the displayed dialog box, you can invite existing accounts to join your organization.

Figure 4-16 Invitations



----End

Viewing Creation Requests

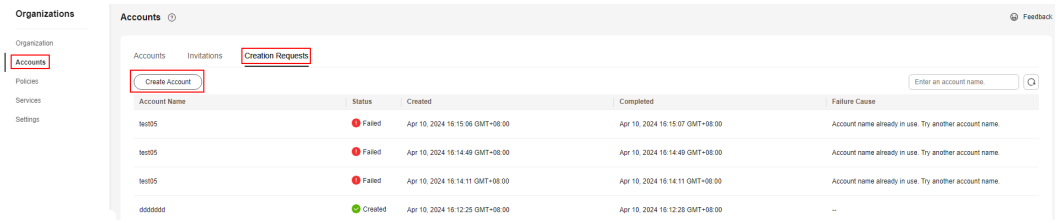
Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Accounts** page, click the **Creation Requests** tab.

You can view the details about account creation requests.

Step 3 Click **Create Account** in the upper left corner of the list. In the displayed dialog box, you can create new accounts for your organization.

Figure 4-17 Creation requests



----End

5 Managing SCPs

5.1 Overview of an SCP

5.1.1 SCP Introduction

Definition

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. The organization management account can use SCPs to limit which permissions can be assigned to member accounts to ensure that they stay within your organization's access control guidelines. SCPs can be attached to an organization, OUs, and member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU.

Helpful links:

- **SCP Principles**: SCP types, how SCPs work, inheritance of SCPs, and relationship between SCPs and IAM policies
- **SCP Syntax**: SCP structure and parameters

Testing SCP Effects

Before applying an SCP to your production environment, it is strongly recommended that you use test accounts in a test environment first to perform thorough system design and testing. This helps avoid any unpleasant surprises in the production environment. After the SCP has been fully verified in the test environment, you can create an OU and move one or a few accounts into it at a time, to ensure that the use of resources is not inadvertently interrupted.

CAUTION

Do not detach the system-defined SCP **FullAccess** unless you replace it with a custom policy with allowed actions. **If you detach FullAccess and configure a custom policy with allowed actions, you must configure actions required by services as well as iamToken::* and signin::*.**

- If you detach the FullAccess SCP from the root OU, the operations for all accounts in the organization will fail. Exercise caution when detaching the FullAccess SCP because this operation is very risky.
- If you detach the FullAccess SCP from an OU, the operations for the accounts in that OU and its lower-level OUs will fail.
- If you detach the FullAccess SCP from a member account, the operations for that account will fail.

Tasks Not Restricted by SCPs

You cannot use SCPs to restrict the following tasks:

- Any action performed by the organization management account or IAM users.
- Any action performed using permissions that are attached to a service-linked agency
- Any API calls made by SCP-unsupported cloud services to SCP-supported cloud services For SCP-supported cloud services and regions, see **Cloud Services for Using SCPs** and **Regions for Using SCPs**.
- Token obtained by APIs used for access to APIs of SCP-supported cloud services (in most cases).

5.1.2 SCP Principles

SCP Types

SCPs are classified as either system-defined policies or custom policies, depending on who creates them.

- **System-defined policies**

System-defined policies refer to commonly used SCPs predefined by Huawei Cloud services for Organizations. An organization administrator can directly use these policies when attaching SCPs to OUs or accounts. Such policies cannot be modified. For details about available SCP system policies, see **System-defined SCPs**.

- **Custom policies**

If system-defined policies cannot meet your requirements, you can use the management account to create and modify custom SCPs based on the actions supported by each service. Custom policies extend and supplement system-defined policies. You can create custom policies for Organizations in a policy editor or JSON view.

SCP Effects on Permissions

- **Permissions boundaries**

  SCPs do not actually grant any permissions to an entity. They only set permissions boundaries for the entity. When SCPs are attached to an OU or a member account, they 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 member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs. Users cannot perform any actions that are denied by SCPs even if the actions are granted to the users by IAM policies.

  Suppose that an SCP is attached to a member account. The SCP allows action A but denies action B. The member account then can grant its IAM users the permission to perform action A but not action B. Even if the permission to perform action B is assigned, the permission cannot be applied.

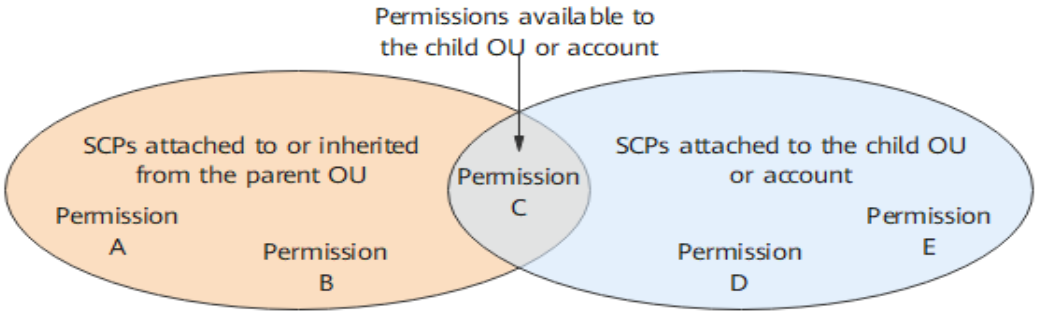
- **Permissions intersection**

  The final effective permissions of an OU or account are the intersection of the permissions of its own SCPs and the allowed SCPs of its parent OU.

  In the following figure, the oval on the left represents an SCP attached to the parent OU. It allows permissions A, B, and C. The oval on the right represents an SCP attached to the child OU or account. It allows permissions C, D, and E. Because the SCP attached to the parent OU does not allow permission D or E, no child OUs or accounts under the parent OU can use them. Even though the SCP attached to the child OU explicitly allows permissions D and E, they are blocked by the SCP attached to the parent OU. Because the SCP attached to the child OU or account does not allow permission A or B, those permissions are blocked for the child OU or account. In this case, the child OU or account can actually use the permission (permission C in the following figure) in the intersection of its own permissions and the allowed permissions of its parent OU.

  If the entity in the set on the right represents a member account, the set of maximum permissions that can be granted to the users and user groups in that account is the intersection of the two sets. If the entity represents a child OU, then the set of maximum permissions that can be granted to that OU is the intersection of the two sets.

  Figure 5-1 How SCPs work

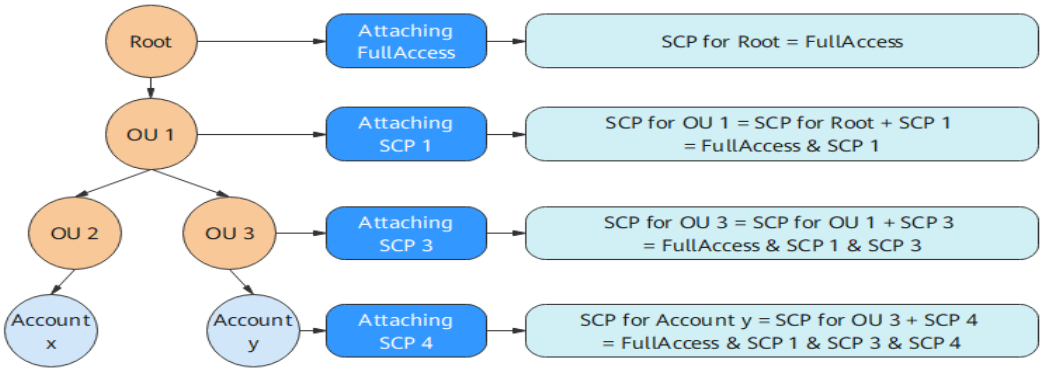


- **Policy inheritance**

  SCPs for an OU or account can be attached directly or inherited from the root OU or the parent OU. When you attach an SCP to a specific OU, all child OUs

and accounts under that OU will inherit that policy. The permissions boundaries of an account or an OU are determined by a combination of the SCPs attached to all upper-level OUs and the SCPs directly attached to the account or OU. In the following figure, Account y is nested in OU 3, and its permissions boundary is jointly determined by the SCPs inherited from the root OU and the SCPs attached to OU 1 and OU 3 as well as Account y.

Figure 5-2 Example SCP inheritance



If you want to allow a service action at the member account level, you must allow that action at every level between the member account and the root OU of your organization. Specifically, you must attach SCPs that allow the given action to every level from the root OU to the member account. You can use either a deny list or an allow list.

- A deny list: This strategy makes use of the **FullAccess** SCP that is attached by default to every OU and account. This SCP overrides the default implicit Deny and allows all permissions to flow down from the root OU to every account, unless you explicitly deny a permission with an additional SCP that you create and attach to the appropriate OU or account. This strategy adheres to the rule that an explicit Deny always overrides any Allow. No account below the level of the OU with the deny policy can use the denied action, and there is no way to add the permission back lower in the hierarchy.
- An allow list: This strategy has you remove the FullAccess SCP that is attached by default to every OU and account. This means that no actions are permitted anywhere unless you explicitly allow them. To allow a service action in an account, you must create your own SCPs and attach them to the account and every OU above it, up to and including the root OU. Every SCP in the hierarchy, starting at the root OU, must explicitly allow the actions that you want to be usable in the OUs and accounts below it. This strategy adheres to the rule that an explicit Allow in an SCP overrides an implicit Deny.

- **Deny preceded**

  When multiple SCPs are attached to an OU or an account, a Deny statement always overrides an Allow statement. Suppose that two SCPs are attached to a member account, one allowing for full access and the other denying access to view billing information. As the Deny statement overrides the Allow statement, the member account is prohibited from viewing the bill. For details, see **Differences Between Explicit Deny and Implicit Deny**.

- **Allow by default**

  When SCPs are enabled for an organization, the **FullAccess** policy is attached by default to all OUs and accounts unless you attach explicit deny policies to the OUs or accounts.

Differences Between Explicit Deny and Implicit Deny

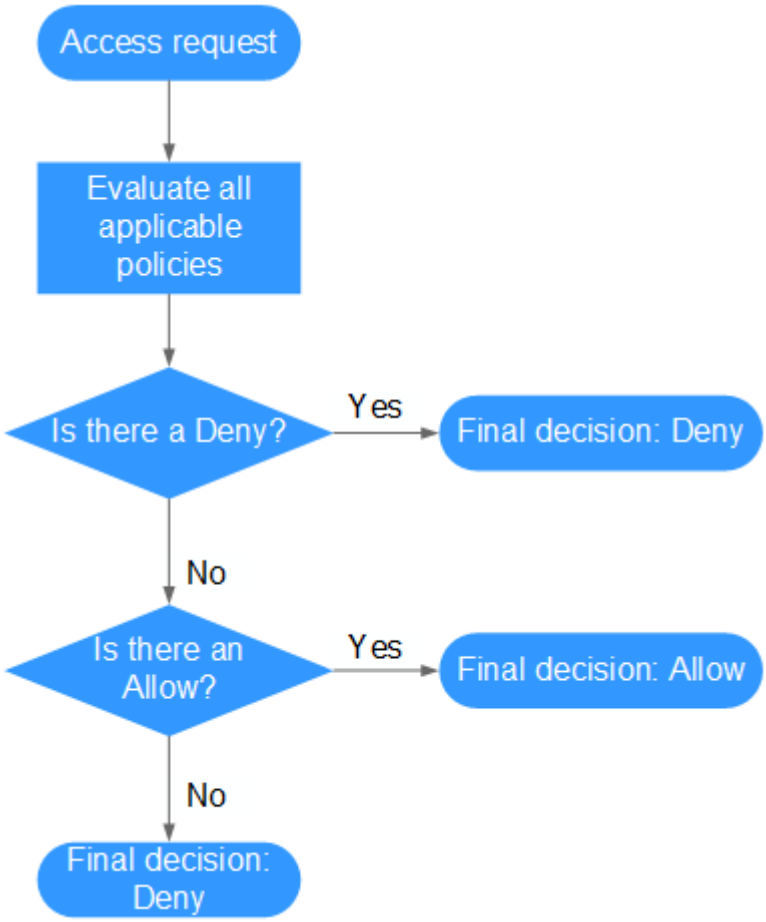
There are two policy effects: Allow and Deny.

If there are no applicable Deny statements but also no applicable Allow statements, all requests are denied by default. This is called an implicit deny. If a policy includes an Allow statement for a given permission and no other policies include a Deny statement for that permission, the Allow statement is applied.

If a policy includes an applicable Deny statement, requests will be denied. This is called an explicit deny. An explicit Deny always takes precedence over Allow. For example, if the SCP of an OU allows permissions A, B, and C, but the SCP of one of its child OU allows permissions A and B but denies permission C, then no accounts in the child OU or accounts in lower-level OUs can use permission C.

The following figure shows the logic for authenticating an access request.

Figure 5-3 Authentication logic



1. A principal sends an access request.

2. The system looks for a Deny statement that applies to the request. If the system finds an applicable Deny, it returns a final decision of Deny, and the authentication ends.
3. If no applicable Deny is found, the system looks for an Allow that would apply to the request. If the system finds an applicable Allow, it returns a final decision of Allow, and the authentication ends.
4. If no applicable Allow is found, the system returns a final decision of Deny, and the authentication ends.

5.1.3 SCP Syntax

The following uses a custom policy for RAM as an example to describe the SCP syntax.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
       "ForAnyValue:StringNotEquals": {
          "g:RequestTag/owner": [
            "Alice",
            "Jack"
          ]
        }
      }
    }
  ]
}
```

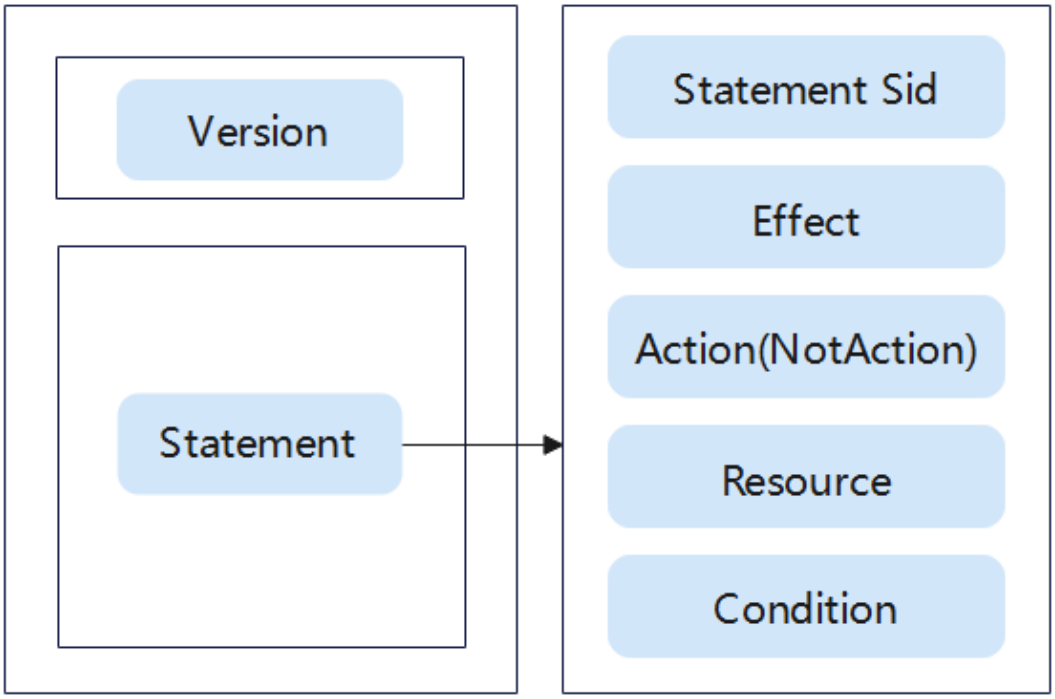
NOTE

SCPs use a similar syntax to that used by IAM identity policies.

Policy Structure

A policy consists of a version and a single statement or an array of individual statements, each indicating a different action.

Figure 5-4 Policy structure



Policy Elements

The following table describes the policy elements (**Version** and **Statement**).

Table 5-1 Policy elements

Element		Mandatory	Description	Value
Version		Yes	Policy version.	5.0 (cannot be customized)
Statement: Permissions defined by a policy	Statement ID (Sid)	No	Identifier of a policy statement. You can assign a Sid value for each statement in a statement array.	A user-defined character string
	Effect	Yes	Determines whether to allow or deny the operations defined in an action.	• **Allow** • **Deny** **NOTE** • If an action has both Allow and Deny effects, the Deny effect takes precedence. • If an action has the Allow effect, the Condition element is not allowed.

Element		Mandatory	Description	Value
	Action	Mandatory for Allow statements Either Action or NotAction for Deny statements	Operations that the SCP allows or denies.	Format: "*Service name*:*Resource type*:*Operation*". Wildcard characters (*) are supported, indicating all options. The wildcard characters (*) and (?) in an element can be used only by itself or at the end of the string. They cannot be used at the beginning or middle of the string. For example, **vpc:subnets:list** indicates the permission to view the VPC subnet list, where **vpc** is the service name, **subnets** refers to the resource type, and **list** is the action.
	NotAction	Not available for Allow statements. Either Action or NotAction for Deny statements.	Operations or services that are exempt from the SCP. A Deny statement denies all operations except those in the NotAction list.	In the same format as Action

Element		Mandatory	Description	Value
	Condition	Not available for Allow statements.	Determines when a policy is in effect. A condition consists of a **condition key** and a **condition operator**.	Format: "*Condition operator*:{*Condition key*:[*Value 1*,*Value 2*]}" If you configure multiple conditions, the policy can be applied only when all the conditions are met. Example: **"StringEndWithIfExists":{"g:UserName":["specialCharactor"]}**: This statement is valid for users whose names end with **specialCharactor**.
	Resource	No If this element is not specified, * is used by default, indicating that the SCP applies to all resources.	Resources that the SCP applies to.	The value can only be * for Allow statements. The value can be either * or a specific resource for Deny statements. Format: *Service name*:region:domain ID:*Resource type*:*Resource path*. Wildcard characters (*) are supported, indicating all resources. Example: "ecs:*:*:instance:*", representing all ECS instances.

NOTE

The following elements are not supported in SCPs:

- Principal
- NotPrincipal
- NotResource

Condition Keys

A condition key is a key in the **Condition** element of a statement. 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, Organizations automatically obtains user information and authenticates users.
- Service-specific condition keys (with the abbreviation of a service name as the prefix, for example, **ram:**) apply only to operations of that service. For details, see the service-specific condition keys of each service in **Actions Supported by SCP-based Authorization**.

Table 5-2 Common global condition keys

Global Condition Key	Type	Description
g:CalledVia	String array	Used to control access across services. When a principal initiates an access request to a cloud service, the service may forward the request to another service. The g:CalledVia key contains a list of services in the chain that send requests on behalf of the principal. This condition key is present when the service forwards the access request of the principal. This condition key is not present when the principal accesses the service directly. See an example in **1**.
g:CalledViaFirst	String	Similar to g:CalledVia, it refers to the first element in the g:CalledVia key, which means the first service that forwards a request on behalf of the principal.
g:CalledViaLast	String	Similar to g:CalledVia, it refers to the last element in the g:CalledVia key, which means the last service that forwards a request on behalf of the principal.
g:CurrentTime	Time	Time when a request is received. It is in ISO 8601 format, for example, 2012-11-11T23:59:59Z. See an example in **2**.
g:DomainName	String	Account name of the requester.
g:DomainId	String	Account ID of the requester.

Global Condition Key	Type	Description
g:EnterpriseProjectId	String	ID of the enterprise project for the request or the requested resource. This condition key is present when the ID of the enterprise project for the request or the requested resource is passed in the API request and the action supports g:EnterpriseProjectId. This condition key is used in authentication, rather than a filter condition. This means resources in the enterprise project specified by this condition key will not be filtered out. See an example in **3**.
g:MFAPresent	Boolean	Whether to use multi-factor authentication (MFA) to obtain STS security tokens. This condition key is true only when you log in to the console through MFA or when you use the assumed-agency session obtained through MFA to make a request. This condition key is present only when a request is sent using STS Security Token. See an example in **4**.
g:MFAAge	Numeric	Validity period of STS security tokens obtained through MFA authentication. This condition key is present only when you log in to the console through MFA authentication or when you use the assumed-agency session obtained through MFA to make a request. The unit is second.
g:PrincipalAccount	String	Same as g:DomainId.
g:PrincipalUrn	String	URN of the requesting principal. Different principals have different URN formats. IAM users: iam::<domain-id>:user:<user-name> IAM assumed-agency sessions: sts::<domain-id>:assumed-agency:<agency-name>/<session-name> Virtual federated users: sts::<domain-id>:external-user:<idp-id>/<session-name> See an example in **5**.
g:PrincipalIsRootUser	Boolean	Whether the requesting principal is an IAM root user. This condition key is present in all requests.
g:PrincipalIsService	Boolean	Whether the requesting principal is a cloud service. You can use this condition key to control whether only cloud services can access the specified APIs.

Global Condition Key	Type	Description
g:PrincipalOrgId	String	ID of the organization that the requesting principal belongs to. You can use this condition key to control access to the specified APIs only from identities in the specific organization. This condition key is present only when the requesting principal is part of an organization. See an example in **6**.
g:PrincipalOrgManagementAccountId	String	ID of the management account in the organization that the requesting principal belongs to. This condition key is present only when the requesting principal is part of an organization. See an example in **7**.
g:PrincipalOrgPath	String	Path of the organization that the requesting principal belongs to. You can use this condition key to control access to the specified APIs only from accounts within the specified organization root or organizational units (OUs). This condition key is present only when the requesting principal is part of an organization. See an example in **8**. An account's organization path is in the following format: <organization-id>/<root-id>/(<ou-id>/)*<account-id>
g:PrincipalServiceName	String	Requesting principal's name. This condition key is present only when the requesting principal is a cloud service. See an example in **9**.
g:PrincipalTag/<tag-key>	String	Tag contained in the requesting principal. The <tag-key> is case insensitive. This condition key is present only when the requesting principal is a tagged IAM user or trust agency, or an assumed-agency session with a session tag. See an example in **10**.
g:PrincipalType	String	Type of the requesting principal, which can be **User**, **AssumedAgency**, or **ExternalUser**. When an IAM user is used for access, the value is **User**. When an IAM assumed-agency session is used for access, the value is **AssumedAgency**. When a virtual federated user is used for access, the value is **ExternalUser**.
g:Referer	String	HTTP referer header in a request. As this condition key is specified by the client, it should not be used to prevent unauthorized access.

Global Condition Key	Type	Description
g:RequestedRegion	String	Region called in a request. If the requested cloud service is a region-specific service, set this condition key to the corresponding region ID, for example, cn-north-4. This condition key is present only when certain region-specific services are requested.
g:RequestTag/<tag-key>	String	Tag contained in a request. The <tag-key> is case insensitive. If a requester passes a tag when calling an API (for example, for adding a tag to an existing resource, or adding a tag during resource creation), you can use this condition key to check whether the request contains the tag. This condition key is present only when the action supports g:RequestTag/<tag-key> and tags are passed in the API request. For more information, see **Actions Supported by SCP-based Authorization**. See an example in **11**.
g:ResourceAccount	String	Requested resource owner's account ID. This condition key is present only in actions of cloud services that support fine-grained permissions management. For more information, see **Actions Supported by SCP-based Authorization**. See an example in **12**.
g:ResourceOrgId	String	ID of the organization that the requested resource account belongs to. This condition key is present only in actions of cloud services that support fine-grained permissions management and the resource owner account is part of an organization. For more information, see **Actions Supported by SCP-based Authorization**. See an example in **13**.
g:ResourceOrgPath	String	Path in the organization that the requested resource account belongs to. This condition key is present only in actions of cloud services that support fine-grained permissions management and the resource owner account is part of an organization. For more information, see **Actions Supported by SCP-based Authorization**. See an example in **14**.

Global Condition Key	Type	Description
g:ResourceTag/<tag-key>	String	Tag contained in the requested resource. The tag key <tag-key> is case insensitive. You can use this condition key to control that only resources with specified tags attached can be accessed. This condition key is present only when the action supports g:ResourceTag/<tag-key> and tags are attached to the requested resources. For more information, see **Actions Supported by SCP-based Authorization**. See an example in **15**.
g:SecureTransport	Boolean	Whether the request is sent using SSL.
g:SourceAccount	String	Account of the resource making a service-to-service request in cross-service access scenarios. This condition key is present only when the action supports g:SourceAccount. It should only be used in resource policies where the cloud service is the principal. See an example in **16**.
g:SourceUrn	String	URN of the resource making a service-to-service request. This condition key is present only when the action supports g:SourceUrn. It should only be used in resource policies where the cloud service is the principal. See an example in **17**.
g:SourceIdentity	String	The **source_identity** field specified when a user obtains IAM temporary credentials through the AssumeAgency API of STS for the first time. This field cannot be changed during subsequent agency switches. This condition key is present only when a request with **source_identity** specified is sent using STS Security Token. See an example in **18**.
g:SourceIp	IP	Source IP address from a public network. See an example in **19**. **NOTE** If the request is initiated within a VPC and passes through a VPC endpoint, g:VpcSourceIp would be used instead of g:SourceIp. This condition key is present only if the access is not initiated through a VPC endpoint. This condition key can be used as a valid access control condition only when the access is initiated through a public network. It does not take effect when a cloud service uses an agency to initiate access on behalf of a user without going through a public network.
g:SourceVpc	String	ID of the VPC from which the request is sent. This condition key is present only when the request is initiated within a VPC and passes through a VPC endpoint to access a cloud service that is configured as a VPC endpoint service.

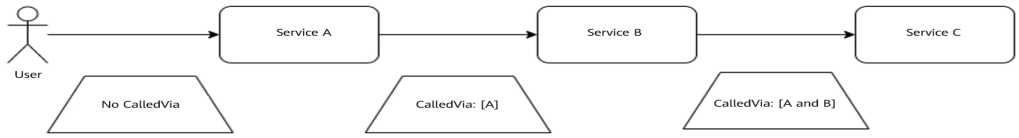
Global Condition Key	Type	Description
g:SourceVpce	String	ID of the VPC endpoint that initiates the request. This condition key is present only when the request is initiated within a VPC and passes through a VPC endpoint to access a cloud service that is configured as a VPC endpoint service. See an example in **20**.
g:TagKeys	String array	List of tag keys in a request. This condition key is present only when the action supports g:TagKeys and tags are passed in the API request.
g:TokenIssueTime	Time	Time when STS Security Token in the access credentials is issued. This condition key is present only when a request is sent using STS Security Token.
g:UserAgent	String	HTTP User-Agent header in a request. As this condition key is specified by the client, it should not be used to prevent unauthorized access.
g:PrincipalId	String	ID of the requesting principal. Different principals have different ID formats. IAM users: <user-id> IAM assumed-agency sessions: <agency-id>:<session-name> Virtual federated users: <idp-id>:<session-name>
g:UserName	String	Name of an IAM user. This condition key is present only when the requester is an IAM user.
g:UserId	String	ID of an IAM user. This condition key is present only when the requester is an IAM user.
g:ViaService	Boolean	Whether the request is initiated by access forwarding from a cloud service on behalf of a principal. The value of this condition key is **true** only when **g:CalledVia** is not an empty string. This condition key is present only when a request is sent using STS Security Token.
g:VpcSourceIp	IP	Source IP address of a request initiated in a VPC. This condition key is present only when the request is initiated within a VPC and passes through a VPC endpoint to access a cloud service that is configured as a VPC endpoint service.

1. **g:CalledVia**

   For example, a user makes a request to service A. Service A then makes a request to service B on behalf of the user, and service B makes a request to service C on behalf of the user. The request received by service A does not

contain the g:CalledVia condition key because the requesting principal is a user. In the request received by service B, g:CalledVia contains the service principal of service A because the request is made by service A on behalf of the user. In the request received by service C, the g:CalledVia contains the service principals of service A and service B, and the sequence is the same as that of the forwarding access request chain. In this case, g:CalledViaFirst is the service principal of service A, and g:CalledViaLast is the service principal of service B. The g:CalledViaFirst and g:CalledViaLast condition keys can be used to specify the first and last services that are called in the forwarding access chain.

Figure 5-5 g:CalledVia application scenario



NOTE

When the user makes a request to a cloud service through the management console, CalledVia contains **service.console**.

For example, the following policy prevents the requests initiated on the management console from calling the RAM API for querying resource shares.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "ram:resourceShares:search"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "ForAnyValue:StringEquals": {
            "g:CalledVia": "service.console"
         }
      }
   }]
}
```

2. **g:CurrentTime**

   For example, the following policy prevents the invocation of cloud service APIs from March 1, 2023 to March 30, 2023.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["ram:resourceShares:search"],
            "Resource": ["*"],
            "Condition": {
                "DateGreaterThan": {"g:CurrentTime": "2023-03-01T00:00:00Z"},
                "DateLessThan": {"g:CurrentTime": "2023-03-30T23:59:59Z"}
            }
        }
```



```
    ]
}
```

3. **g:EnterpriseProjectId**

   This condition key is used in authentication. For example, the following policy prevents users from querying VPC permissions by enterprise project, and only denies access with **enterprise_project_id** set to **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx** in the request for calling the GET /v1/{project_id}/vpcs API.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "vpc:vpcs:list"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "StringEquals": {
            "g:EnterpriseProjectId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
         }
      }
   }]
}
```

   NOTE

   The g:EnterpriseProjectId condition key is not a filtering condition. This means resources in the enterprise project specified by this condition key will not be filtered out. In the example for calling the GET /v1/{project_id}/vpcs API, when **enterprise_project_id** is **all_granted_eps**, the VPCs associated with all enterprise projects of the user are queried. If this policy has been configured for the user, the VPCs associated with the enterprise project specified by **g:EnterpriseProjectId** in the policy will not be queried.

4. **g:MFAPresent**

   This condition key is present only when a request is sent using STS Security Token. If a request is sent using permanent credentials, this condition key is not present.

   For example, the following identity policy only allows API calling by principals authenticated using multi-factor authentication (MFA). The IfExists operator is used to cover scenarios where the g:MFAPresent condition key is not present when requests are made using permanent credentials.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "*"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "BoolIfExists": {
            "g:MFAPresent": "false"
         }
      }
   }]
}
```

5. **g:PrincipalUrn**

For example, the following SCP prevents the user **yyy** from creating resource shares.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "ram:resourceShares:create"
      ],
      "Condition": {
         "StringEquals": {
            "g:PrincipalUrn": "iam::xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:user:yyy"
         }
      }
   }]
}
```

6. **g:PrincipalOrgId**

   For example, the following policy prevents the accounts in organization **o-xxxxxxxxxxx** from calling the API for searching resource shares in RAM.

```
{
    "Version": "5.0",
    "Statement": [
       {
           "Effect": "Deny",
           "Action": ["ram:resourceShares:search"],
           "Resource": ["*"],
           "Condition": {
              "StringEquals": {
              "g:PrincipalOrgID": "o-xxxxxxxxxx"

              }
           }
       }
    ]
}
```

7. **g:PrincipalOrgManagementAccountId**

   For example, the condition key value **xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx** in the following identity policy matches the management account ID in the request.

```
{
   "Condition": {
      "StringEquals": {
         "g:PrincipalOrgManagementAccountId": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
      }
   }
}
```

8. **g:PrincipalOrgPath**

   For example, the condition key value **ou-qqq** in the following identity policy matches the organizational units (OUs) that the requesting principal belongs to in the request.

```
{
   "Condition": {
      "StringMatch": {
         "g:PrincipalOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/*"
      }
   }
}
```

   For example, the condition key value **ou-qqq** in the following identity policy matches any child OUs that the requesting principal belongs to in the request.

```
{
   "Condition": {
```



```
        "StringMatch": {
            "g:PrincipalOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/ou-*"
        }
    }
}
```

9. **g:PrincipalServiceName**

   For example, the condition key value **service.RAM** in the following policy matches the principal that is making the request.

```
{
    "Condition": {
        "StringEquals": {
            "g:PrincipalServiceName": "service.RAM"
        }
    }
}
```

10. **g:PrincipalTag/<tag-key>**

    For example, the following policy prevents IAM users tagged with {"department": "hr"} from accessing IAM APIs.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "iam:*"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringEquals": {
                "g:PrincipalTag/department": "hr"
            }
        }
    }]
}
```

11. **g:RequestTag/<tag-key>**

    For example, the following policy prevents users from creating resource shares tagged with {"team": "engineering"}.

```
{
    "Version": "5.0",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["ram:resourceShares:create"],
            "Resource": ["*"],
            "Condition": {
                "StringEquals": {
                    "g:RequestTag/team": "engineering"
                }
            }
        }
    ]
}
```

12. **g:ResourceAccount**

    For example, the following identity policy prevents users from using KMS keys of other than the specified users to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
```



```
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "g:ResourceAccount": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
            }
        }
    }]
}
```

13. **g:ResourceOrgId**

    For example, the following identity policy prevents users from using KMS keys of other than the specified organizations to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringNotEquals": {
                "g:ResourceOrgId": "o-xxxxxxxx"
            }
        }
    }]
}
```

14. **g:ResourceOrgPath**

    For example, the following policy prevents users from using KMS keys of the accounts in the **ou-qqq** OU to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "StringMatch": {
                "g:ResourceOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/*"
            }
        }
    }]
}
```

    For example, the following policy prevents users from using KMS keys of the accounts in the child OUs under the **ou-qqq** OU to decrypt data.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "kms:cmk:decryptData"
        ],
        "Resource": [
            "*"
        ],
```



```
      "Condition": {
         "StringMatch": {
            "g:ResourceOrgPath": "o-xxx/r-yyy/ou-zzz/ou-qqq/ou-*"
         }
      }
   }]
}
```

15. **g:ResourceTag/<tag-key>**

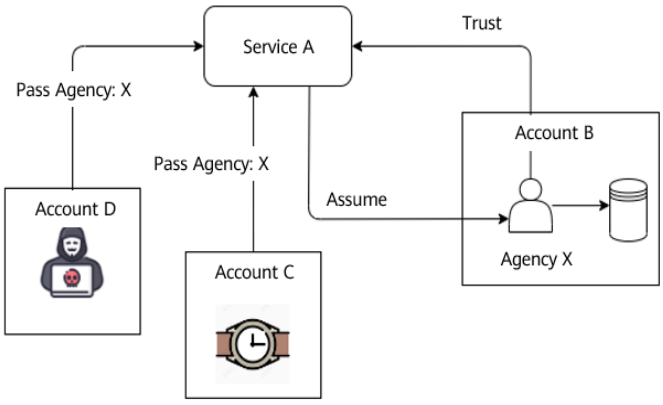
    For example, the following policy prevents users from modifying resource shares tagged with {"team": "engineering"}.

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [
    "ram:resourceShares:delete",
    "ram:resourceShares:update"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "g:ResourceTag/team": "engineering"
    }
   }
  }
 ]
}
```

16. **g:SourceAccount**

    For example, service A is used to record activities. It helps a user (account B) to dump activity logs triggered by a device (account C) to a specified OBS bucket. To enable service A to write data into the bucket, the administrator of account B creates an agency or trust agency named X for service A to manage OBS buckets under account B. After account B or account C accesses service A and triggers a request, service A obtains the temporary identity credentials of the specified agency or trust agency X and writes data to the bucket.

    Figure 5-6 Confused deputy



The agency or trust agency name X is not confidential. If an attacker (account D) obtains the agency name and triggers service A in the same way, the activity records of the attacker would be incorrectly recorded in the OBS bucket. The attacker uses service A's agency to indirectly modify the OBS bucket of account B. This is called the confused deputy.

The g:SourceAccount condition key is used to control the account of the resource making a service-to-service request. The following policy only allows service A to switch to the assumed-agency session for account **xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx** or **yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy**.

```
{
   "Version": "5.0",
   "Statement": [{
      "Principal": {
         "Service": [
            "Service.A"
         ]
      },
      "Action": [
         "sts:agencies:assume"
      ],
      "Condition": {
         "StringEquals": {
            "g:sourceAccount": [
               "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx",
               "yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy"
            ]
         }
      }
   }]
}
```

17. **g:SourceUrn**

    Similar to g:SourceAccount, this condition key is also used to solve the confused deputy issue. Assume that user devices (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx) are defined as watches and bracelets. The g:SourceUrn condition key is used to control the URN of the resource making a service-to-service request. The following policy only allows service A to switch to the corresponding assumed-agency session for the watch or bracelet that meets the conditions.

    ```
    {
       "Version": "5.0",
       "Statement": [{
          "Principal": {
             "Service": [
                "Service.A"
             ]
          },
          "Action": [
             "sts:agencies:assume"
          ],
          "Condition": {
             "StringEquals": {
                "g:sourceUrn": [
                   "alarm:*:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:watch:*",
                   "alarm:*:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx:bracelet:*"
                ]
             }
          }
       }]
    }
    ```

18. **g:SourceIdentity**

For example, the following policy prevents principals whose **source_identity** is **yyyyy** from switching the agency.

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Principal": {
            "IAM": [
                "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
            ]
        },
        "Action": [
            "sts:agencies:assume"
        ],
        "Condition": {
            "StringEquals": {
                "g:SourceIdentity": "yyyyy"
            }
        }
    }]
}
```

19. **g:SourceIp**

    For example, the following policy denies the programmatic or console access to KMS from source IP addresses within the xxx.xx.xx.0/24 range.

    NOTICE

    The source IP address must be a public IP address. Do not include a private IP address in the condition key.

    ```
    {
        "Version": "5.0",
        "Statement": [{
            "Effect": "Deny",
            "Action": [
                "kms:cmk:decryptData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "IpAddress": {
                    "g:SourceIp": "xxx.xx.xx.0/24"
                }
            }
        }]
    }
    ```

    The following condition keys in the initial request context will not be passed in subsequent requests forwarded by the service on behalf of the principal: g:SourceIp, g:SourceVpce, g:SourceVpc, and g:VpcSourceIp. As a result, when these condition keys are used to control access permissions, requests forwarded by the cloud service on behalf of the principal may be denied. In practice, you are advised to use g:CalledVia to forward access requests.

    There is an exception: The public network access initiated by the principal from the console can be regarded as a programmatic access of the principal from the public network, so the request forwarded by the console on behalf of the principal contains the initial g:SourceIp.

For example, the following policy denies the programmatic or console access to KMS from source IP addresses beyond xxx.xx.xx.0/24. In addition, the policy allows cloud services to forward access requests on behalf of the principal.

```
{
   "Version": "5.0",
   "Statement": [{
         "Effect": "Deny",
         "Action": [
            "kms:cmk:decryptData"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "NotIpAddress": {
               "g:SourceIp": "xxx.xx.xx.0/24"
            },
            "Bool": {
               "g:ViaService": "false"
            }
         }
      },
      {
         "Effect": "Deny",
         "Action": [
            "kms:cmk:decryptData"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "NotIpAddress": {
               "g:SourceIp": "xxx.xx.xx.0/24"
            },
            "StringEqualsIfExists": {
               "g:CalledViaFirst": "service.console",
               "g:CalledViaLast": "service.console"
            }
         }
      }
   ]
}
```

20. **g:SourceVpce**

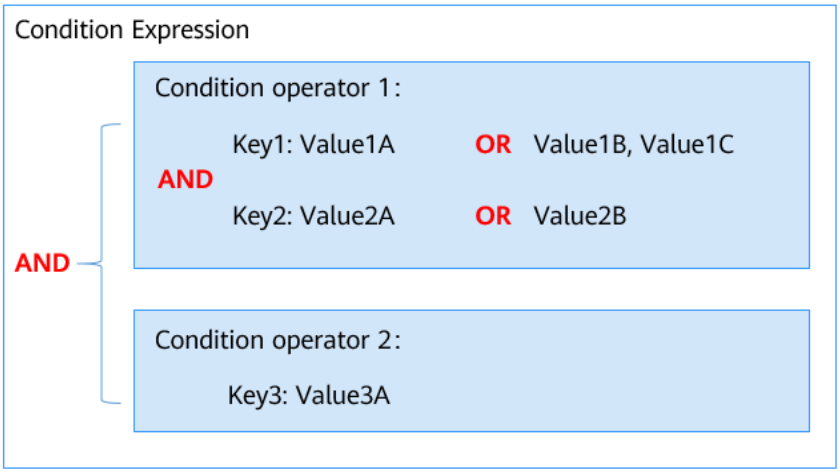
    For example, the following policy denies access to KMS from a VPC endpoint other than **xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**. In addition, the policy allows cloud services to forward access requests on behalf of the principal.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "kms:cmk:decryptData"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "StringNotEquals": {
            "g:SourceVpce": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
         },
         "Bool": {
            "g:ViaService": "false"
         }
      }
   }]
}
```


- Multivalued condition keys
  a. ForAllValues: Tests whether the value of every member of the request set is a subset of the condition key set. The condition returns true if every key value in the request matches at least one value in the policy.
  b. ForAnyValue: Tests whether at least one member of the set of request values matches at least one member of the set of condition key values. The condition returns true if any one of the key values in the request matches any one of the condition values in the policy. The condition returns false if there are no matching keys in the request, or if the key value resolves to an empty data set.

Condition Operators

Figure 5-7 Condition operators



i. If a single condition operator includes multiple values for one key, that condition operator is evaluated using a logical OR. The condition returns **true** if any one of the key values in the request matches any one of the condition values in the policy.

NOTICE

For condition operators that contain Not (such as StringNotEquals), the request value cannot match any of the condition values.

ii. The AND operation is used between different condition keys of the same operator. It is also used between different operators.

Operators

A condition operator, a condition key, and a condition value together constitute a complete condition statement. A policy can be applied only when its request conditions are met. The operator suffix **IfExists** indicates that a policy is applied if a request value is empty or meets the specified condition. For example, if the operator **StringEqualsIfExists** is selected for a policy, the policy is applied if a request value is empty or equal to the specified condition value. Operators are string operators. They are not case-sensitive unless otherwise specified.

- String

Table 5-3 String condition operators

Type	Operator	Description
String	StringEquals	Exact matching, case sensitive
	StringNotEquals	Negated matching, case sensitive
	StringEqualsIgnoreCase	Exact matching, ignoring case
	StringNotEqualsIgnore-Case	Negated matching, ignoring case
	StringMatch	Case-sensitive matching. The values can include multi-character match wildcards (*) and single-character match wildcards (?) anywhere in the string.
	StringNotMatch	Negated case-sensitive matching. The values can include multi-character match wildcards (*) and single-character match wildcards (?) anywhere in the string.

For example, the following policy prevents the requester Tom from deleting or modifying resource shares.

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "ram:resourceShares:delete",
            "ram:resourceShares:update"
         ],
         "Condition": {
            "StringEquals": {
               "g:DomainName": [
                  "Tom"
               ]
            }
         }
      }
   ]
}
```

- Numeric

Table 5-4 Numeric condition operators

Type	Operator	Description
Numeric	NumberEquals	Matching
	NumberNotEquals	Negated matching

Type	Operator	Description
	NumberLessThan	"Less than" matching
	NumberLessThanEquals	"Less than or equals" matching
	NumberGreaterThan	"Greater than" matching
	NumberGreaterThanEquals	"Greater than or equals" matching

- Date

Table 5-5 Date condition operators

Type	Operator	Description
Date	DateLessThan	Matching before a specific date and time
	DateLessThanEquals	Matching at or before a specific date and time
	DateGreaterThan	Matching after a specific date and time
	DateGreaterThanEquals	Matching at or after a specific date and time

For example, the following policy prevents requesters from accessing RAM before August 1, 2022.

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "ram:*:*"
         ],
         "Condition": {
            "DateLessThan": {
               "g:CurrentTime": [
                  "2022-08-01T00:00:00Z"
               ]
            }
         }
      }
   ]
}
```

- Boolean

Table 5-6 Boolean condition operators

Type	Operator	Description
Bool	Bool	Boolean conditions let you construct condition elements that restrict access based on comparing a key to "true" or "false."

- Null

Table 5-7 Null condition operators

Type	Operator	Description
Null	Null	You can use a Null condition operator to check if a condition key is absent at the time of authorization. In the policy statement, you can use either "true" (the key does not exist or is null) or "false" (the key exists and its value is not null).

- IP

Table 5-8 IP condition operators

Type	Operator	Description
IP	IpAddress	IP address or IP address range
	NotIpAddress	All IP addresses beyond a specific IP address or IP address range

For example, the following policy prevents requests from the IP address range (10.27.128.0 to 10.27.128.255) from modifying the specified permanent access keys.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "iam:credentials:updateCredentialV5"
      ],
      "Condition": {
        "IpAddress": {
          "g:SourceIp": [
            "10.27.128.0/24"
          ]
        }
```



```
    }
  }
 ]
}
```

- IfExists operator suffix

  You can add "IfExists" to the end of any condition operator name except the "Null condition", for example, StringEqualsIfExists. If the policy key is present in the context of the request, process the key as specified in the policy. If the key is not present, evaluate the condition element as true.

5.2 Enabling or Disabling the SCP Type

Enabling the SCP Type

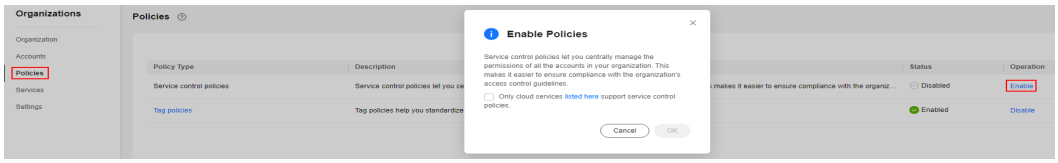
Before you create and attach an SCP to OUs and accounts, you have to enable the SCP type from the organization's management account. After the SCP type is enabled, Organizations automatically attach the FullAccess policy (allowing for all operations) to all OUs and accounts.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Enable** in the **Operation** column of the service control policies.

Step 3 In the displayed dialog box, select the check box and click **OK**.

Figure 5-8 Enabling the SCP type



----End

Disabling the SCP type

If you no longer want to use SCPs to manage permissions for your organization, you can disable the SCP type from the organization's management account.

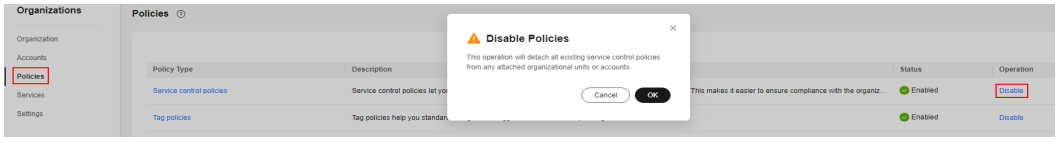
CAUTION

- After the SCP type is disabled in an organization, all SCPs are automatically detached from all OUs and accounts in the organization. However, the SCPs are not deleted.
- If you disable the SCP type and then enable it again, the FullAccess SCP is still attached to all entities in the organization and attachments of other SCPs are lost. If you want to re-enable them, you must re-attach them to the entities.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Disable** in the **Operation** column of the service control policies.

Figure 5-9 Disabling the SCP type



Step 3 Click **OK** in the displayed dialog box.

----End

5.3 Creating an SCP

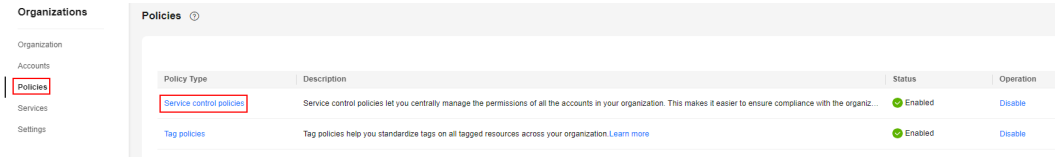
This topic describes how to create a custom SCP. For SCP examples, see **Example SCPs**.

Procedure

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Service control policies**.

Figure 5-10 Accessing the **Service control policies** page



Step 3 Click **Create Policy**.

Figure 5-11 Creating an SCP

Step 4 Enter a policy name. Ensure that you are entering a unique policy name. It must be different from any other existing policy.

(Optional) You can also enter a description for the policy.

Step 5 On the left of the policy content, edit the policy content in JSON.

For details about how to build JSON policy statements, see **SCP Syntax** and **Example SCPs**.

NOTE

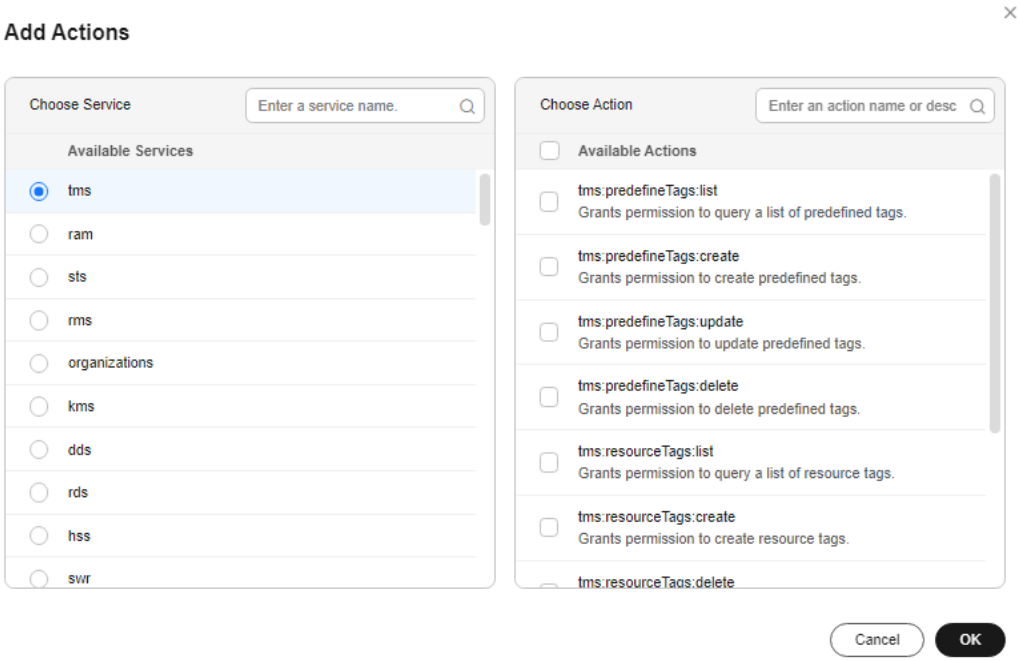
The **Version** value of a custom policy must be **5.0**.

When **Effect** is **Allow**, the Condition element is not allowed, that is, the condition key cannot be added.

Step 6 On the right of the policy content, use the policy editor to edit the actions, resources, and conditions of the custom policy.

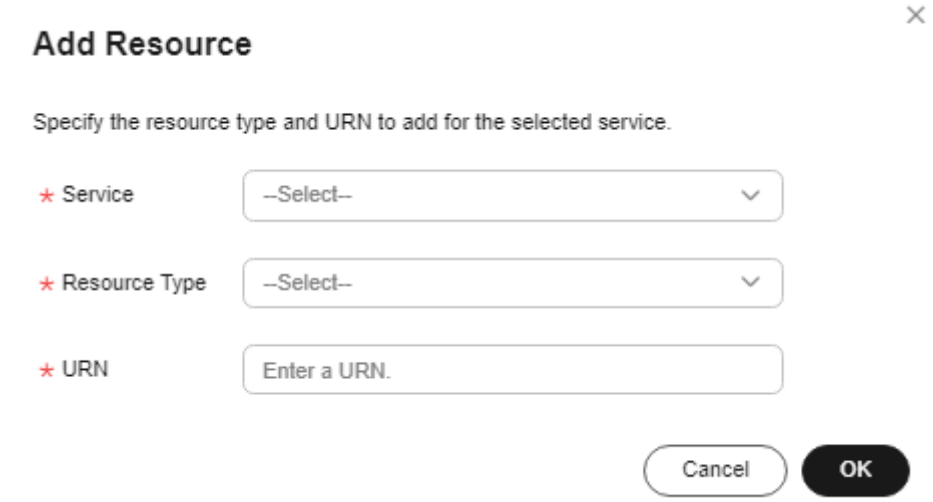
- Adding an action: Click **+** to add an action. The added action will appear under **Available Actions**, as shown in **Figure 5-12**.

Figure 5-12 Adding an action



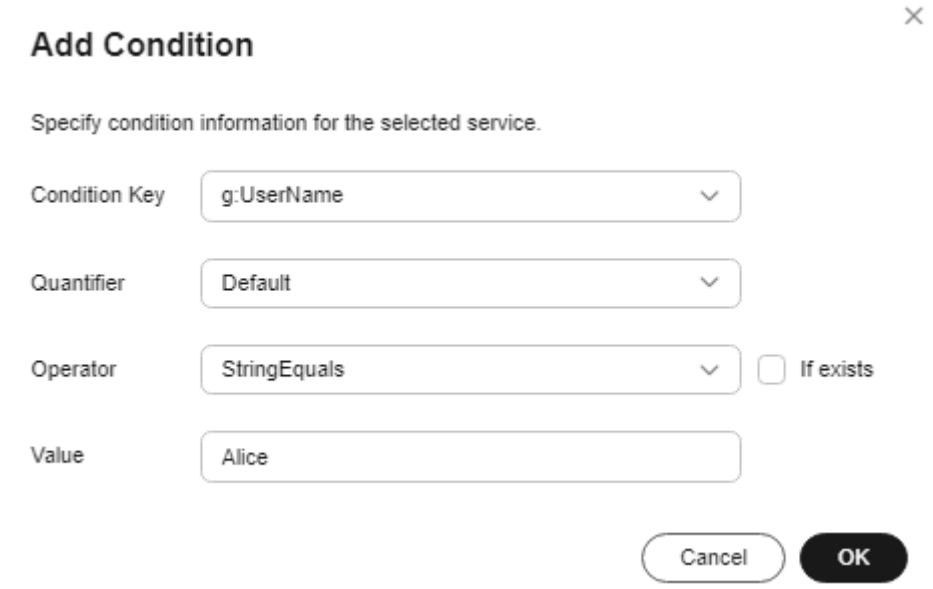
- Adding a resource: Only services available for resource-level authorization can be added. Click **+** to select a service for the action, and enter the URN to identify the specific resource you want to control access to, as shown in **Figure 5-13**.

Figure 5-13 Adding a resource



- (Optional) Add a condition. You can click **+** to add a condition key and an operator to define the conditions for when a policy is in effect, as shown in **Figure 5-14**.

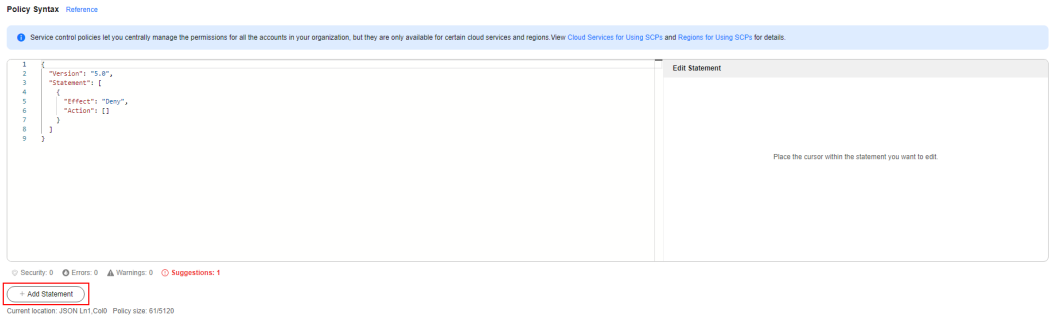
Figure 5-14 Adding a condition



Step 7 (Optional) Click **Add Statement** to add an object for the Statement element.

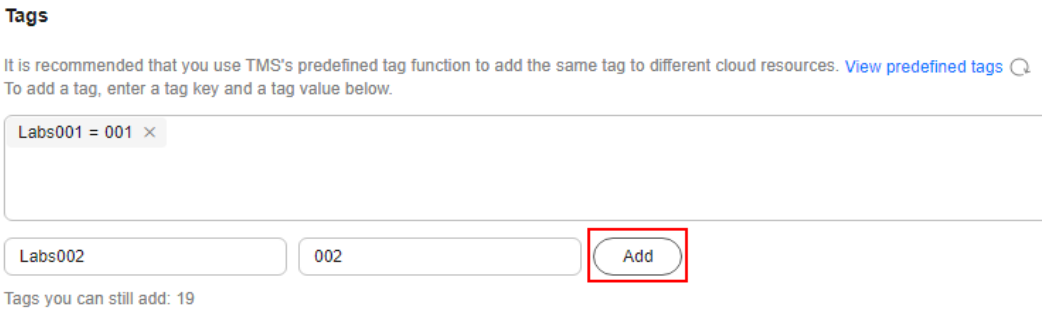
The value for the Statement element can be an array of multiple objects that identify different permissions.

Figure 5-15 Adding a statement



Step 8 (Optional) Add one or more tags. Enter a tag key and a tag value, and click **Add**.

Figure 5-16 Adding tags to the SCP



Step 9 Click **Save**. If the policy list is displayed, the SCP is created successfully. If a message appears indicating incorrect policy content, modify the SCP syntax.

----End

5.4 Modifying or Deleting an SCP

The following describes how to modify and delete a custom SCP.

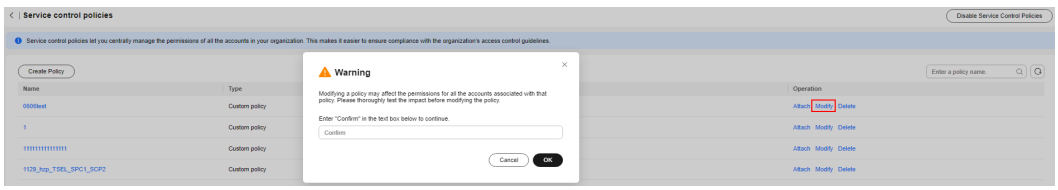
Modifying an SCP

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Service control policies**.

Step 3 Locate the custom SCP you want to modify and click **Edit** in the **Operation** column. In the displayed dialog box, enter "Confirm" and click **OK**.

Figure 5-17 Modifying an SCP



Step 4 On the **Modify Policy** page, modify the policy name and description as needed. , as shown in #org_03_0036/fig977144619493.

Step 5 Edit the policy content if needed. You can use the statement editor to modify the policy syntax. For details, see **SCP Syntax**.

Step 6 Click **Save**. If the policy list is displayed, the SCP is updated successfully. If a message appears indicating incorrect policy content, modify the SCP syntax.

----End

Deleting an SCP

An SCP that is attached to OUs or accounts cannot be deleted. To delete such an SCP, you need to detach the SCP from the OUs or accounts first.

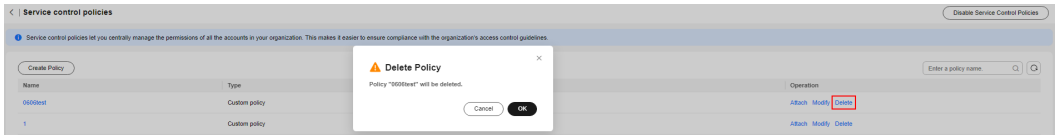
Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Service control policies**.

Step 3 Locate the target custom SCP and click **Delete** in the **Operation** column.

Step 4 Click **OK** in the displayed dialog box.

Figure 5-18 Deleting an SCP



----End

5.5 Attaching or Detaching an SCP

You can attach an SCP to or detach it from the root OU, other OUs or accounts from the organization's management account.

Constraints

- SCPs affect only member accounts in an organization. They have no effect on the management account, IAM users, and agencies.
- SCPs are applied within 30 minutes after they are attached.

Attaching an SCP

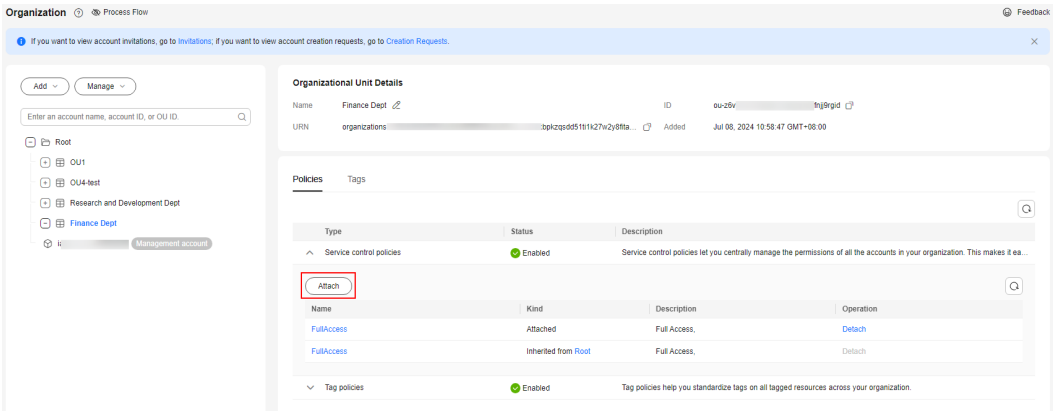
Method 1:

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU or account you want to attach the SCP to.

Step 3 On the details page, click the **Policies** tab. On the page, expand **Service control policies** and click **Attach**.

Figure 5-19 Attaching an SCP



Step 4 Select the policy to be added and enter "Confirm" in the text box. Then, click **Attach**.

----End

Method 2:

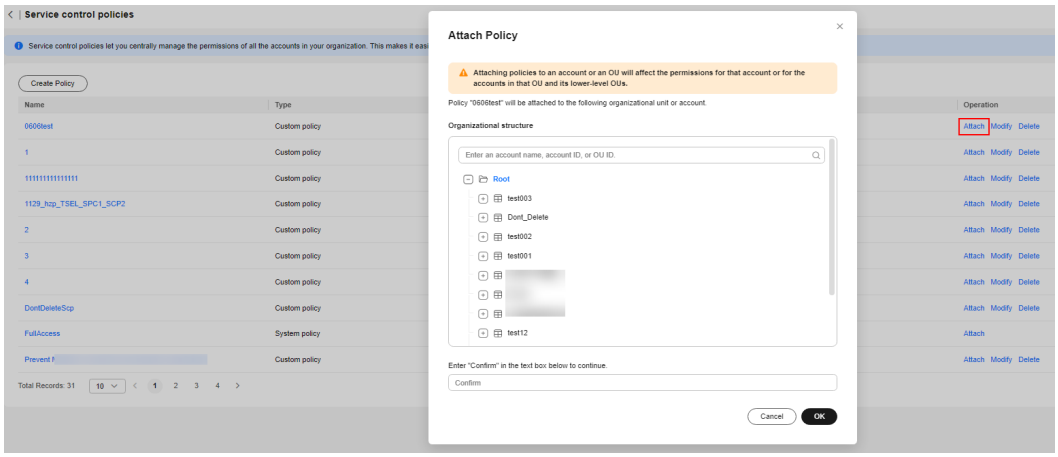
Step 1 Access the **Policies** page on the Organizations console.

Step 2 Click **Service control policies**. The list of SCPs is displayed.

Step 3 Locate the SCP you want to attach and click **Attach** in the **Operation** column. Then, select the OU or account you want to attach the SCP to.

Step 4 In the displayed dialog box, enter "Confirm" and click **OK**.In the displayed dialog box, click **OK**.

Figure 5-20 Attaching an SCP



----End

Detaching an SCP

Method 1:

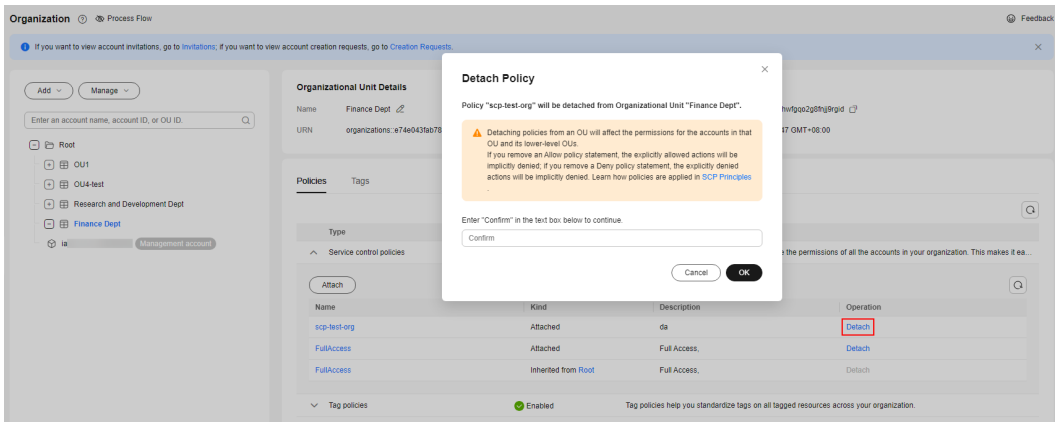
Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU or account you want to detach the SCP from.

Step 3 On the details page, click the **Policies** tab. On the page, expand **Service control policies**, locate the target SCP and click **Detach** in the **Operation** column.

Step 4 In the displayed dialog box, enter "Confirm" and click **OK**.In the displayed dialog box, click **OK**.

Figure 5-21 Detaching an SCP



NOTE

You cannot detach the last SCP from an OU or account. There must be at least one SCP attached to every OU or account.

----End

Method 2:

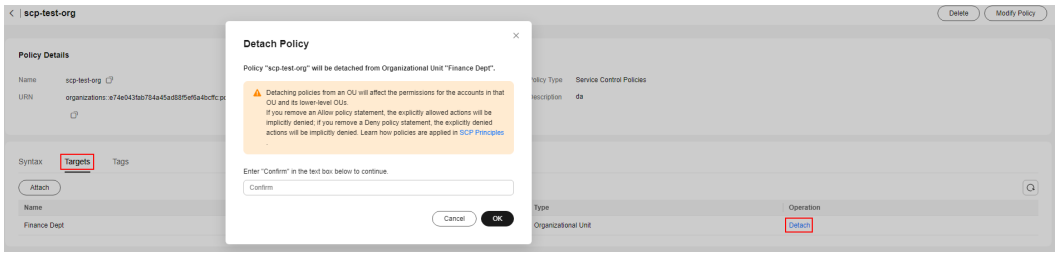
Step 1 Access the **Policies** page on the Organizations console.

Step 2 Click **Service control policies**. The list of SCPs is displayed.

Step 3 Click the name of the target SCP and click the **Targets** tab.

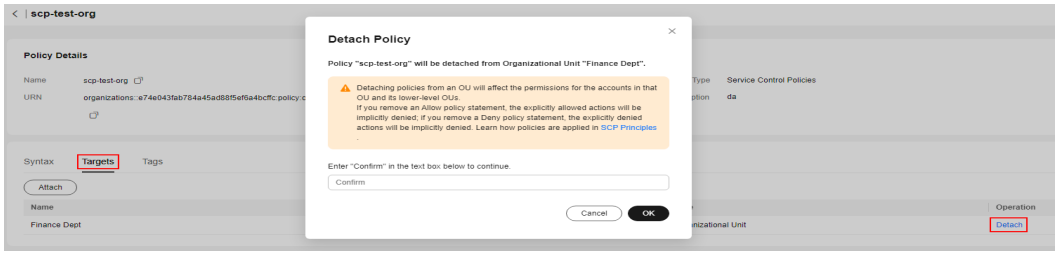
Step 4 Locate the OU or account that you want to detach the SCP from and click **Detach** in the **Operation** column.

Figure 5-22 Detaching an SCP



Step 5 In the displayed dialog box, enter "Confirm" and click **OK**.In the displayed dialog box, click **OK**.

Figure 5-23 Detaching an SCP



----End

5.6 Example SCPs

This section provides some example SCPs for your reference, including:

- **Preventing Member Accounts from Leaving an Organization**
- **Blocking Service Access for the Root User**
- **Prohibiting Creation of Resources with Specified Tags**
- **Prohibiting Access to Specified Regions**
- **Preventing Sharing with Accounts Outside an Organization**
- **Preventing Sharing Specified Resource Types**
- **Preventing Aggregation Authorization to Accounts Outside the Current Organization**
- **Preventing the Root User from Using Cloud Services Other Than IAM**
- **Preventing IAM Users and Agencies from Making Certain Changes**
- **Preventing IAM Users and Agencies from Making Specified Changes, with an Exception for Specified Accounts**

Preventing Member Accounts from Leaving an Organization

The following SCP prevents member accounts from leaving an organization.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "organizations:organizations:leave"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Blocking Service Access for the Root User

The following SCP blocks access to the specified actions for the root user in a member account. If you want to restrict access in specific ways, you can modify the Action and Resource elements.

```
{
  "Version": "5.0",
```



```
 "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "ecs:*:*"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "BoolIfExists": {
        "g:PrincipalIsRootUser": "true"
      }
    }
  }
 ]
}
```

Prohibiting Creation of Resources with Specified Tags

The following SCP prevents users from creating resource shares with the {"team": "engineering"} tag. If you want to prevent resource creation in specific ways, you can modify the Action, Resource, and Condition elements.

```
{
    "Version":"5.0",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":["ram:resourceShares:create"],
            "Resource":["*"],
            "Condition":{
                "StringEquals":{
                    "g:RequestTag/team":"engineering"
                }
            }
        }
    ]
}
```

Prohibiting Access to Specified Regions

The following SCP prevents users from accessing all ECS resources in **regionid1** but not in any other regions. If you want to restrict access in specific ways, you can modify the Action, Resource, and Condition elements.

This SCP applies only to region-specific services. **regionid1** in the SCP is only an example for you reference. Enter the specific region ID you want when using this SCP.

```
{
    "Version":"5.0",
    "Statement":[
        {
            "Effect":"Deny",
            "Action":["ecs:*:*"],
            "Resource":["*"],
            "Condition":{
                "StringEquals":{
                    "g:RequestedRegion":"regionid1"
                }
            }
        }
    ]
}
```


Preventing Sharing with Accounts Outside an Organization

The following SCP prevents accounts within an organization from sharing resources with accounts outside the organization. You are advised to attach this SCP to the root OU of the organization so that the SCP will be applied to the entire organization.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create",
        "ram:resourceShares:associate"

      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringNotLike": {
          "ram:TargetOrgPaths": [
            "organization_id/root_id/ou_id" [Note: Enter the path ID of the organization.]
          ]
        }
      }
    }
  ]
}
```

Preventing Sharing Specified Resource Types

The following SCP prevents accounts from sharing VPC subnets. You can modify the resource type in the Condition element of the SCP statement as required.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "ram:RequestedResourceType": [
            "vpc:subnet" [Note: You can change the resource type as required.]
          ]
        }
      }
    }
  ]
}
```

Preventing Aggregation Authorization to Accounts Outside the Current Organization

The following SCP prevents accounts within an organization from granting aggregation authorization to accounts outside the organization. You are advised to attach this SCP to the root OU of your organization to prevent accounts outside

your organization from collecting information about the resources of accounts in your organization. You can also attach this SCP to source accounts to prevent them from accepting authorization requests from the aggregator account.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:aggregationAuthorizations:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:AuthorizedAccountOrgPath": [
            "organization_id/root_id/ou_id" [Note: Enter the path ID of the organization.]
          ]
        }
      }
    }
  ]
}
```

Preventing the Root User from Using Cloud Services Other Than IAM

The following SCP prevents the root user from using any cloud services other than IAM.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "NotAction": [
        "iam:*:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Bool": {
          "g:PrincipalIsRootUser": [
            "true"
          ]
        }
      }
    }
  ]
}
```

Preventing IAM Users and Agencies from Making Certain Changes

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization.

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:resourceShares:update",
        "ram:resourceShares:delete",
```



```
      "ram:resourceShares:associate",
      "ram:resourceShares:disassociate",
      "ram:resourceShares:associatePermission",
      "ram:resourceShares:disassociatePermission"
    ],
    "Resource": [
      "ram::*:resourceShare:resource-id"
    ]
  }
 ]
}
```

Preventing IAM Users and Agencies from Making Specified Changes, with an Exception for Specified Accounts

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization except for specified accounts.

```
{
 "Version": "5.0",
 "Statement": [
  {
   "Effect": "Deny",
   "Action": [
    "ram:resourceShares:update",
    "ram:resourceShares:delete",
    "ram:resourceShares:associate",
    "ram:resourceShares:disassociate",
    "ram:resourceShares:associatePermission",
    "ram:resourceShares:disassociatePermission"
   ],
   "Resource": [
    "ram::*:resourceShare:resource-id"
   ],
   "Condition": {
    "StringNotEquals": {
     "g:DomainId": [
      "account-id" [Note: Enter the ID of the account to deny.]
     ]
    }
   }
  }
 ]
}
```

5.7 System-defined SCPs

The following table lists the SCPs preconfigured on Huawei Cloud.

Table 5-9 Huawei Cloud SCPs

Policy	Description
FullAccess	Allows all permissions on all resources.

NOTE

At least one SCP must be attached to each root, OU, and account.

5.8 Cloud Services for Using SCPs

SCPs are available for the following cloud services:

NOTE

Cloud services for using SCPs also support IAM identity policies.

Compute

No.	Service Name	Reference
1	Elastic Cloud Server (ECS)	Elastic Cloud Server (ECS)
2	Bare Metal Server (BMS)	Bare Metal Server (BMS)
3	Image Management Service (IMS)	Image Management Service (IMS)
4	Auto Scaling	Auto Scaling (AS)

Storage

No.	Service Name	Reference
1	Cloud Backup and Recovery (CBR)	Cloud Backup and Recovery (CBR)
2	Elastic Volume Service (EVS)	Elastic Volume Service (EVS)
3	Scalable File Service Turbo (SFS Turbo)	Scalable File Service Turbo (SFS Turbo)

Networking

No.	Service Name	Reference
1	Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC)
2	Elastic IP (EIP)	Elastic IP (EIP)
3	NAT Gateway (NAT)	NAT Gateway
4	Elastic Load Balance (ELB)	Elastic Load Balance (ELB)
5	VPC Endpoint (VPCEP)	VPC Endpoint (VPCEP)
6	Direct Connect	Direct Connect (DC)
7	Enterprise Router	Enterprise Router (ER)

No.	Service Name	Reference
8	Global Accelerator	Global Accelerator (GA)
9	Cloud Connect	Cloud Connect (CC)

Containers

No.	Service Name	Reference
1	Cloud Container Engine (CCE)	Cloud Container Engine (CCE)
2	Software Repository for Container (SWR)	SoftWare Repository for Container (SWR)

Analytics

No.	Service Name	Reference
1	Data Lake Insight (DLI)	Data Lake Insight (DLI)
2	DataArts Studio	DataArts Studio
3	GaussDB(DWS)	GaussDB(DWS)
4	MapReduce Service (MRS)	MapReduce Service (MRS)
5	Cloud Search Service (CSS)	Cloud Search Service (CSS)

Content Delivery & Edge Computing

No.	Service Name	Reference
1	Content Delivery Network (CDN)	Content Delivery Network (CDN)

Databases

No.	Service Name	Reference
1	Relational Database Service (RDS)	Relational Database Service (RDS)
2	Document Database Service (DDS)	Document Database Service (DDS)
3	GaussDB	GaussDB

No.	Service Name	Reference
4	Data Replication Service (DRS)	**Data Replication Service (DRS)**
5	TaurusDB	**TaurusDB**

Security & Compliance

No.	Service Name	Reference
1	Cloud Native Anti-DDoS Basic (Anti-DDoS)	**Cloud Native Anti-DDoS Basic (Anti-DDoS)**
2	Cloud Native Anti-DDoS Advanced (CNAD)	**Cloud Native Anti-DDoS Advanced (CNAD)**
3	Advanced Anti-DDoS (AAD)	**Advanced Anti-DDoS (AAD)**
4	Data Encryption Workshop (DEW), including the following sub-services: • Key Management Service (KMS) • Cloud Secret Management Service (CSMS) • Key Pair Service (KPS) • Dedicated Hardware Security Module (Dedicated HSM)	**Data Encryption Workshop (DEW)**
5	Host Security Service (HSS)	**Host Security Service (HSS)**
6	SecMaster	**SecMaster**
7	Cloud Firewall (CFW)	**Cloud Firewall (CFW)**
8	Data Security Center (DSC)	**Data Security Center (DSC)**
9	Private Certificate Authority (PCA)	**Private Certificate Authority (PCA)**
10	SSL Certificate Manager (SCM)	**SSL Certificate Manager (SCM)**
11	Cloud Bastion Host (CBH)	**Cloud Bastion Host (CBH)**
12	Database Security Service (DBSS)	**Database Security Service (DBSS)**
13	Web Application Firewall (WAF)	**Web Application Firewall (WAF)**

IoT

No.	Service Name	Reference
1	IoT Device Access (IoTDA)	**IoT Device Access (IoTDA)**

Middleware

No.	Service Name	Reference
1	Distributed Cache Service (DCS)	**Distributed Cache Service (DCS)**
2	Cloud Service Engine (CSE)	**Cloud Service Engine (CSE)**
3	API Gateway	**API Gateway (APIG)**

Developer Services

No.	Service Name	Reference
1	ServiceStage	**ServiceStage**
2	CodeArts	**CodeArts**
3	CodeArts Pipeline	**CodeArts Pipeline**
4	CodeArts PerfTest	**CodeArts PerfTest**

Business Applications

No.	Service Name	Reference
1	Domain Name Service (DNS)	**Domain Name Service (DNS)**
2	Workspace	**Workspace**

Management & Governance

No.	Service Name	Reference
1	Simple Message Notification (SMN)	**Simple Message Notification (SMN)**
2	Log Tank Service (LTS)	**Log Tank Service (LTS)**
3	Identity and Access Management (IAM)	**Identity and Access Management (IAM)**

No.	Service Name	Reference
4	Security Token Service (STS)	**Security Token Service (STS)**
5	Resource Formation Service (RFS)	**Resource Formation Service (RFS)**
6	IAM Identity Center	**IAM Identity Center**
7	Organizations	**Organizations**
8	Resource Access Manager (RAM)	**Resource Access Manager (RAM)**
9	Enterprise Project Management Service (EPS)	**Enterprise Project Management Service (EPS)**
10	Tag Management Service (TMS)	**Tag Management Service (TMS)**
11	Config (original service name: RMS)	**Config**
12	IAM Access Analyzer	**IAM Access Analyzer**
13	Cloud Trace Service (CTS)	**Cloud Trace Service (CTS)**
14	Resource Governance Center (RGC)	**Resource Governance Center (RGC)**
15	Application Operations Management (AOM)	**Application Operations Management (AOM)**
16	Cloud Eye	**Cloud Eye (CES)**

User Support

No.	Service Name	Reference
1	Billing Center	**Billing Center**
2	Cost Center	**Cost Center**
3	My Account	**My Account**
4	Enterprise Center	**Enterprise Center**
5	Message Center	**Message Center**
6	Customer Operations Capabilities	**Customer Operation Capabilities**

Migration

No.	Service Name	Reference
1	Object Storage Migration Service (OMS)	Object Storage Migration Service (OMS)
2	Server Migration Service (SMS)	Server Migration Service (SMS)

5.9 Regions for Using SCPs

SCPs are available in the following regions:

NOTE

Regions for using SCPs also support the use of IAM identity policies.

Table 5-10 Regions for using SCPs

Region Name	Region Code
AP-Singapore	ap-southeast-3
AP-Bangkok	ap-southeast-2
AP-Jakarta	ap-southeast-4
CN East-Shanghai1	cn-east-3
CN East-Shanghai2	cn-east-2
CN-Hong Kong	ap-southeast-1
CN North-Beijing1	cn-north-1
CN North-Beijing4	cn-north-4
CN South-Guangzhou	cn-south-1
CN North-Ulanqab1	cn-north-9
CN Southwest-Guiyang1	cn-southwest-2
CN East-Qingdao	cn-east-5
TR-Istanbul	tr-west-1
AF-Johannesburg	af-south-1
LA-Mexico City1	na-mexico-1
LA-Mexico City2	la-north-2
LA-Sao Paulo1	sa-brazil-1
LA-Santiago	la-south-2

Region Name	Region Code
ME-Riyadh	me-east-1
AF-Cairo	af-north-1
CN East2	cn-east-4

5.10 Actions Supported by SCP-based Authorization

5.10.1 Compute

5.10.1.1 Elastic Cloud Server (ECS)

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.

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 ECS, 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 ECS, see **Conditions**.

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

Table 5-11 Actions supported by ECS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ecs:cloudServers:createServers	Grants permission to create ECSs.	write	-	• g:RequestTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys • ecs:imageID • ecs:FlavorId • ecs:VpcId • ecs:SubnetId • ecs:PortId • ecs:KmsKeyId • eip:AssociatePublicIp • ecs:AvailabilityZone • evs:Encrypted • cbr:VaultId • ecs:SSHKeyPairName • ecs:SupportAgentType • ecs:ImageSupportAgentType • ecs:ImageType • ecs:OsVersion • ecs:OsType • ecs:ImagePlatform

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ecs:cloudServers:deleteServers	Grants permission to delete ECSs.	write	instance *	-
ecs:cloudServers:resize	Grants permission to modify ECS specifications.	write	instance *	ecs:FlavorId -
ecs:cloudServers:attachSharedVolume	Grants permission to attach a specified shared EVS disk to multiple ECSs in a batch.	write	instance *	• evs:Encrypted • ecs:KmsKeyId • ecs:VolumeId evs:Encrypted
ecs:cloudServers:showServer	Grants permission to query ECS details.	read	instance *	-
ecs:cloudServers:attach	Grants permission to attach disks to an ECS.	write	instance *	• evs:Encrypted • ecs:KmsKeyId • ecs:VolumeId evs:Encrypted
ecs:cloudServers:listServerBlockDevices	Grants permission to query information about the disks attached to an ECS.	list	instance *	-
ecs:cloudServers:showServerBlockDevice	Grants permission to query information about a single disk attached to an ECS.	read	instance *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ecs:cloudServers:updateServerBlockDevice	Grants permission to modify information about a single disk attached to an ECS.	write	instance *	-
ecs:cloudServers:changeOS	Grants permission to change the ECS OS.	write	instance *	• ecs:imageID • evs:Encrypted • ecs:KmsKeyId • ecs:SSHKeyPairName • ecs:ImageType • ecs:OsVersion • ecs:OsType • ecs:ImagePlatform
ecs:cloudServers:detachVolume	Grants permission to detach disks from an ECS.	write	instance *	-
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 *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ecs:cloudServers:showResetPasswordFlag	Grants permission to query whether one-click password reset is supported.	read	instance *	-
ecs:cloudServers:showServerPassword	Grants permission to get the password for logging in to an ECS.	read	instance *	-
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:rebuild	Grants permission to reinstall the ECS OS.	write	instance *	• evs:Encrypted • ecs:KmsKeyId • ecs:SSHKeyPairName evs:Encrypted
ecs:cloudServers:vnc	Grants permission to obtain the VNC login address.	read	instance *	-
ecs:cloudServers:updateServer	Grants permission to modify ECS information.	write	instance *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ecs:cloudServers:addNics	Grants permission to add NICs to an ECS in a batch.	write	instance *	• eip:AssociatePublicIp • ecs:SubnetId • ecs:PortId -
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:batchCreateServerTags	Grants permission to add tags to an ECS in a batch.	write	instance *	• g:RequestTag/<tag-key> • g:TagKeys
ecs:cloudServers:batchDeleteServerTags	Grants permission to delete tags from an ECS in a batch.	write	instance *	• g:RequestTag/<tag-key> • g:TagKeys
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 *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ecs:cloudServers:listServersDetails	Grants permission to query ECS details.	list	-	g:EnterpriseProjectId
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:resetServerPwd	Grants permission to reset the password of an ECS.	write	instance *	-
ecs:cloudServers:listServerGroups	Grants permission to query ECS groups.	list	-	-
ecs:cloudServers:createServerGroup	Grants permission to create ECS groups.	write	-	-
ecs:cloudServers:showServerGroup	Grants permission to query ECS groups.	read	-	-
ecs:cloudServers:deleteServerGroup	Grants permission to delete ECS groups.	write	-	-
ecs:cloudServers:addServerGroupMember	Grants permission to add ECSs to an ECS group.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ecs:cloudServers:deleteServerGroupMember	Grants permission to delete ECSs from an ECS group.	write	-	-
ecs:cloudServers:listResizeFlavors	Grants permission to query the target ECS flavors to which a flavor can be changed.	list	-	-
ecs:cloudServers:listServerTags	Grants permission to query project tags.	list	-	-

Each API of ECS usually supports one or more actions. **Table 5-12** lists the supported actions and dependencies.

Table 5-12 Actions and dependencies supported by ECS APIs

API	Action	Dependencies
POST /v1.1/{project_id}/cloudservers	ecs:cloudServers:createServers	• eip:publicIps:create • eip:publicIps:associateInstance • iam:agencies:pass • eip:bandwidths:insertPublicIps
POST /v1/{project_id}/cloudservers	ecs:cloudServers:createServers	• eip:publicIps:create • eip:publicIps:associateInstance • iam:agencies:pass • eip:bandwidths:insertPublicIps

API	Action	Dependencies
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
GET /v1/{project_id}/cloudservers/{server_id}	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}/cloudservers/{server_id}/metadata	ecs:cloudServers:updateMetadata	iam:agencies:pass
DELETE /v1/{project_id}/cloudservers/{server_id}/metadata/{key}	ecs:cloudServers:deleteMetadata	-
POST /v1/{project_id}/cloudservers/{server_id}/migrate	ecs:cloudServers:migrate	-
GET /v1/{project_id}/cloudservers/{server_id}/os-interface	ecs:cloudServers:listServerInterfaces	-

API	Action	Dependencies
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}/reinstallos	ecs:cloudServers:rebuild	-
POST /v2/{project_id}/cloudservers/{server_id}/reinstallos	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	-
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	-
PUT /v1/{project_id}/cloudservers/{server_id}	ecs:cloudServers:updateServer	-
POST /v1/{project_id}/cloudservers/{server_id}/nics	ecs:cloudServers:addNics	-

API	Action	Dependencies
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	-
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/{server_id}/os-reset-password	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	-

API	Action	Dependencies
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	-
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/actions/change-charge-mode	ChangeServerChargeMode	• billing:order:pay • billing:subscription:renew
GET /v1/{project_id}/cloudservers/flavor-sell-policies?flavor_id={flavor_id}	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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-13**, 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 ECS.

Table 5-13 Resource types supported by ECS

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

Conditions

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, ecs:) only apply to operations of the ECS service. For details, see **Table 5-14**.
  - 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.

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

Table 5-14 Service-specific condition keys supported by ECS

Condition Key	Type	Single-valued/ 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:SSHKeyPairName	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.
ecs:ImageSupportAgentType	string	Multivalued	Filters access based on the supported image agent type in the request parameter.

Condition Key	Type	Single-valued/ Multivalued	Description
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.

5.10.1.2 Bare Metal Server (BMS)

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.

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 BMS, 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 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 following table lists the actions that you can define in SCP statements for BMS.

Table 5-15 Actions supported by BMS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
bms:servers:updateBaremetalServer	Grants permission to modify BMSs.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:showBaremetalServerInterfaceAttachments	Grants permission to query BMS NICs.	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
bms:servers:resetServerPwd	Grants permission to reset a BMS password with a few clicks.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:showResetPasswordFlag	Grants permission to check whether BMS passwords can be reset with a few clicks.	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:showWindowsBaremetalServerPwd	Grants permission to obtain Windows BMS passwords.	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:deletePassword	Grants permission to delete Windows BMS passwords.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:showBaremetalServerVolumeInfo	Grants permission to query EVS disks attached to a BMS.	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
bms:servers:create	Grants permission to create BMSs.	write	-	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key> • eip:AssociatePublicIp • bms:Flavorld • bms:VpcId • bms:SubnetId • bms:KmsKeyId • evs:Encrypted • bms:ImageId • bms:SSHKeyPairName • bms:AvailabilityZone • bms:VolumeType
bms:servers:showBaremetalServer	Grants permission to query details about a BMS.	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
bms:servers:attachVolume	Grants permission to attach EVS disks to a BMS.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • bms:KmsKeyId • evs:Encrypted • bms:VolumeType • bms:VolumeId
bms:servers:detachVolume	Grants permission to detach EVS disks from a BMS.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:updateMetadata	Grants permission to update BMS metadata.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:reInstallOS	Grants permission to reinstall a BMS OS.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • bms:KmsKeyId • evs:Encrypted • bms:SSHKeyPairName
bms:servers:showBaremetalServerTags	Grants permission to query BMS tags.	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
bms:servers:start	Grants permission to start BMSs in a batch.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:reboot	Grants permission to restart BMSs in a batch.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:stop	Grants permission to stop BMSs in a batch.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:list	Grants permission to query BMS details.	list	-	g:EnterpriseProjectId
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:batchCreateBaremetalServerTags	Grants permission to add tags in a batch.	write	instance*	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
bms:servers:batchDeleteBaremetalServerTags	Grants permission to delete tags in a batch.	write	instance*	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
bms:servers:addNics	Grants permission to bind NICs to a BMS.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • eip:AssociatePublicIp • bms:SubnetId
bms:server:deleteNics	Grants permission to unbind NICs from a BMS.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:servers:serialConsole	Grants permission to obtain an address for remotely logging in to a BMS.	read	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
bms:server:updateInterface	Grants permission to modify BMS NICs.	write	instance*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Each API of BMS usually supports one or more actions. **Table 5-16** lists the supported actions and dependencies.

Table 5-16 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	-

API	Action	Dependencies
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	-
POST /v1/{project_id}/baremetalservers	bms:servers:create	eip:publicIps:create eip:publicIps:associateInstance iam:agencies:pass eip:bandwidths:insertPublicIps -
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	-
POST /v1/{project_id}/baremetalservers/{server_id}/reinstallos	bms:servers:reInstallOS	-

API	Action	Dependencies
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	-
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	-
PUT /v1/{project_id}/baremetalservers/{server_id}/os-interface/{port_id}	bms:server:updateInterface	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-17**, 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 BMS.

Table 5-17 Resource types supported by BMS

Resource Type	URN
instance	bms:<region>:<account-id>:instance:<server-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.
- <server-id>: indicates the ID of the BMS on which operations will be performed.

Conditions

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 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, **bms:**) apply only to operations of the BMS service. For details, see **Table 5-18**.
  - 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.

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

Table 5-18 Service-specific condition keys supported by BMS

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

5.10.1.3 Image Management Service (IMS)

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.

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.
- **Resource Type** 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 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 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 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 following table lists the actions that you can define in SCP statements for IMS.

Table 5-19 Supported Actions

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ims:images:list	Grants permission to view images.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ims:images:get	Grants permission to view details about a specified image.	read	image *	-
ims:images:create	Grants permission to create image metadata.	write	-	• g:RequestTag/<tag-key> • g:TagKeys
ims:images:share	Grants permission to share images.	permission_management	image *	ims:TargetOrgPaths
ims:images:copyInRegion	Grants permission to replicate images within a region.	write	image *	ims:Encrypted
ims:images:copyCrossRegion	Grants permission to replicate images across regions.	write	image *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
ims:quotas:get	Grants permission to query the image quota.	read	-	-
ims:images:upload	Grants permission to upload images.	write	image *	-
ims:wholeImages:create	Grants permission to create full-ECS images.	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:export	Grants permission to export images.	read	image *	-
ims:dataImages:create	Grants permission to create data disk images from external image files.	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ims:serverImages:create	Grants permission to create images.	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:setTags	Grants permission to update image tags.	tagging	image *	• g:RequestTag/<tag-key> • g:TagKeys
ims:images:getTags	Grants permission to query tags of an image.	read	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:deleteImage	Grants permission to delete an image.	write	image *	-
ims:images:updateImage	Grants permission to update image information.	write	image *	-
ims:images:listOsVersion	Grants permission to query OSs supported by images.	list	-	-
ims:images:getJob	Grants permission to query progresses of asynchronous tasks.	read	-	-
ims:images:import	Grants permission to import images.	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
ims:images:setOrDeleteTags	Grants permission to add or deleting image tags in a batch.	write	-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ims:images:updateMemberStatus	Grants permission to update the status of members who can use shared images.	write	image *	-
ims:images:addMember	Grants permission to add a tenant that can use a shared image.	write	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ims:images:deleteMember	Grants permission to delete a tenant from the group where the members can use a shared image.	write	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ims:images:listImagesByTag	Grants permission to query images by tag.	read	-	-
ims:images:showImageTags	Grants permission to query tags of an image.	read	image *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ims:images:listImageTags	Grants permission to query project tags.	list	-	-

Each API of IMS usually supports one or more actions. **Table 5-20** lists the supported actions and dependencies.

Table 5-20 Actions and dependencies supported by IMS APIs

API	Action	Dependencies
GET /v2/cloudimages	ims:images:list	-
GET /v2/images/{image_id}	ims:images:get	-

API	Action	Dependencies
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 PUT /v2/images/{image_id}/file	ims:images:upload	• ims:images:get • ims:images:update
POST /v1/cloudimages/wholeimages/action	ims:wholeImages:create	-
POST /v1/cloudimages/{image_id}/file	ims:images:export	• obs:object:GetObject • obs:object:PutObject
• POST /v2/cloudimages/quickimport/action (required only for quickly importing a data disk image) • POST /v1/cloudimages/dataimages/action	ims:dataImages:create	-
• PATCH /v2/cloudimages/{image_id} (required only for enterprise project migration) • POST /v2/cloudimages/action • POST /v2/cloudimages/quickimport/action (required only for quickly importing a system disk image) • POST /v1/cloudimages/{image_id}/copy (required only by enterprise project users)	ims:serverImages:create	-
PUT /v1/cloudimages/tags	ims:images:setTags	-

API	Action	Dependencies
GET /v1/cloudimages/tags	ims:images:getTags	-
DELETE /v2/images/{image_id}	ims:images:deleteImage	-
• PATCH /v2/cloudimages/{image_id} • PATCH /v2/images/{image_id}	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	• ims:dataImages:create • ims:serverImages:create
POST /v2/{project_id}/images/{image_id}/tags/action	ims:images:setOrDeleteTags	• ims:images:setTags • ims:images:deleteTags
• PUT /v1/cloudimages/members • PUT /v2/images/{image_id}/members/{member_id}	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 SCP applies to. If you specify a resource type for any action in **Table 5-21**, 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 specify in SCP statements for IMS.

Table 5-21 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 SCP 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:**) apply only to operations of IMS. For details, see **Table 5-22**.
  - 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.

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

Table 5-22 Service-specific condition keys supported by IMS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
ims:TargetOrgPaths	string	Multivalued	Filters access based on the **Organizations Path** of the specified sharing account.
ims:Encrypted	boolean	Single valued	Controls operations such as image import and replication based on whether images are encrypted.
ims:TargetBucketOrgPaths	string	Multivalued	Filters access based on the **Organizations Path** of the specified destination bucket owner account.
ims:OriginBucketOrgPaths	string	Multivalued	Filters access based on the **Organizations Path** of the specified source bucket owner account.

5.10.1.4 Auto Scaling (AS)

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 AS, 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 AS, see **Conditions**.

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

Table 5-23 Actions supported by AS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as:scalingGroup:create	Grants permission to create an AS group.	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • as:ScalingConfigId • as:VpcId • as:VpcSubnetId • as:ElbPoolId • as:MaxInstanceSize • as:MinInstanceSize

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as:scalingGroup:delete	Grants permission to delete an AS group.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:list	Grants permission to list AS groups.	list	-	g:EnterpriseProjectId
as:scalingGroup:get	Grants permission to query AS group details.	read	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:update	Grants permission to modify an AS group.	write	-	• g:EnterpriseProjectId • as:ScalingConfigId • as:VpcSubnetId • as:ElbPoolId • as:MaxInstanceSize • as:MinInstanceSize
as:scalingGroup:resume	Grants permission to enable an AS group.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:pause	Grants permission to disable an AS group.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as:scalingConfig:create	Grants permission to create an AS configuration.	write	-	• as:EcsInstanceId • as:EcsInstanceType • as:EcsFlavorId • as:ImageId • as:ImsDiskImageId • as:CbrDiskSnapshotId • as:EcsServerGroupId • as:EvsEncrypted • as:KmsKeyId • as:EvsVolumeType • as:KpsSSHKeyPairName • as:AssociatePublicIp
as:scalingConfig:delete	Grants permission to delete an AS configuration.	write	scalingConfig*	-
as:scalingConfig:batchDelete	Grants permission to delete AS configurations.	write	scalingConfig*	-
as:scalingConfig:list	Grants permission to list AS configurations.	list	scalingConfig*	-
as:scalingConfig:get	Grants permission to query AS configuration details.	read	scalingConfig*	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as:scalingGroup:batchAddInstances	Grants permission to add instances to an AS group.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchRemoveInstances	Grants permission to delete instances from an AS group.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesProtect	Grants permission to enable instance protection for instances.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesUnprotect	Grants permission to disable instance protection for instances.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesStandby	Grants permission to put instances into the standby status.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:batchSetInstancesExitStandby	Grants permission to move instances out of the standby status.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:deleteInstance	Grants permission to delete instances from an AS group.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as:scalingGroup:listInstances	Grants permission to list instances in an AS group.	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingPolicy:create	Grants permission to create an AS policy.	write	-	g:EnterpriseProjectId
as:scalingPolicy:list	Grants permission to list AS policies.	list	-	g:EnterpriseProjectId
as:scalingPolicy:get	Grants permission to query AS policy details.	read	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:update	Grants permission to modify an AS policy.	write	-	g:EnterpriseProjectId
as:scalingPolicy:delete	Grants permission to delete an AS policy.	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:execute	Grants permission to execute an AS policy.	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:resume	Grants permission to enable an AS policy.	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:pause	Grants permission to disable an AS policy.	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:batchPause	Grants permission to disable AS policies.	write	scalingPolicy*	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as:scalingPolicy:batchResume	Grants permission to enable AS policies.	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:batchDelete	Grants permission to delete AS policies.	write	scalingPolicy*	g:EnterpriseProjectId
as:scalingPolicy:listAll	Grants permission to list AS policies of a tenant.	list	-	g:EnterpriseProjectId
as:scalingGroup:listActivityLogs	Grants permission to query scaling action logs.	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingPolicy:listExecuteLogs	Grants permission to query AS policy execution logs.	list	scalingPolicy*	g:EnterpriseProjectId
as::tagResource	Grants permission to add tags.	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
as::untagResource	Grants permission to delete tags.	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
as::listTags	Grants permission to query tags of all resources.	list	-	-
as::listTagsForResource	Grants permission to query tags of a resource.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as::listResourcesByTag	Grants permission to query resources by tag.	list	-	• g:RequestTag/<tag-key> • g:TagKeys
as:scalingGroup:createLifecycleHook	Grants permission to create a lifecycle hook.	write	-	g:EnterpriseProjectId
as:scalingGroup:listLifecycleHooks	Grants permission to list lifecycle hooks.	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:getLifecycleHook	Grants permission to query lifecycle hook details.	read	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:updateLifecycleHook	Grants permission to modify a lifecycle hook.	write	-	g:EnterpriseProjectId
as:scalingGroup:deleteLifecycleHook	Grants permission to delete a lifecycle hook.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:callbackInstanceHook	Grants permission to call back a lifecycle hook.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:listInstanceHooks	Grants permission to query suspended instances.	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
as:scalingGroup:createNotification	Grants permission to create notifications.	write	-	g:EnterpriseProjectId
as:scalingGroup:listNotifications	Grants permission to query notifications.	list	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:deleteNotification	Grants permission to delete notifications.	write	scalingGroup*	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
as:scalingGroup:getQuotas	Grants permission to query instance and AS policy quotas.	read	-	g:EnterpriseProjectId
as::listQuotas	Grants permission to query instance and AS policy quotas.	read	-	-

Each API of AS usually supports one or more actions. **Table 5-24** lists the actions and dependencies supported by AS APIs.

Table 5-24 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	-

API	Action	Dependencies
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	-
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	• as:scalingGroup:batchAddInstances • as:scalingGroup:batchSetInstancesProtect • as:scalingGroup:batchRemoveInstances • as:scalingGroup:batchSetInstancesStandby • as:scalingGroup:batchSetInstancesUnprotect • as:scalingGroup:batchSetInstancesExitStandby	-

API	Action	Dependencies
DELETE /autoscaling-api/v1/{project_id}/scaling_group_instance/{instance_id}	as:scalingGroup:deleteInstance	-
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	• as:scalingPolicy:resume • as:scalingPolicy:pause • as:scalingPolicy:execute	-
POST /autoscaling-api/v1/{project_id}/scaling_policies/action	as:scalingPolicy:batchDelete as:scalingPolicy:batchPause 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	-

API	Action	Dependencies
PUT /autoscaling-api/v2/{project_id}/scaling_policy/{scaling_policy_id}	as:scalingPolicy:update	-
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 SCP applies to. If you specify a resource type for any action in **Table 5-25**, 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 AS.

Table 5-25 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 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, **as:**) only apply to operations of the BMS service. For details, see **Table 5-26**.
  - 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.

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

Table 5-26 Service-specific condition keys supported by AS

Service-specific Condition Key	Type	Single-valued/ 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:MinInstanceSize	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/ 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.

5.10.2 Storage

5.10.2.1 Cloud Backup and Recovery (CBR)

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 IAM permissions can be applied only if they are allowed by the SCPs.

This section describes the elements (Action, Resource, and Condition) used by Organizations SCPs.

- 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 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 SCP 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 SCP policy statements.
  - If this column includes a resource type, you must specify the resource 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 CBR, see **Resources**.
- The **Condition Key** column includes keys that you can specify in the Condition element of an SCP 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 CBR, see **Conditions**.

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

Table 5-27 Supported Actions

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cbr:tasks:list	Grants permission to query the task list.	list	task *	-
			-	g:EnterpriseProjectId
cbr:tasks:get	Grants permission to query a task.	read	task *	g:EnterpriseProjectId
cbr:member:create	Grants permission to add a share member.	permission_management	backup *	g:EnterpriseProjectId
			-	cbr:TargetOrgPaths
cbr:member:update	Grants permission to update the share member status.	write	backup *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cbr:member:get	Grants permission to query share member details.	read	backup *	g:EnterpriseProjectId
cbr:member:list	Grants permission to obtain the share member list.	list	backup *	-
cbr:member:delete	Grants permission to delete a share member.	permission_management	backup *	g:EnterpriseProjectId
cbr:vaults:showCheckpoint	Grants permission to query a restore point.	read	-	-
cbr:vaults:showSummary	Grants permission to query the vault overview.	list	-	-
cbr:vaults:replicate	Grants permission to replicate a restore point.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:backup	Grants permission to create a restore point.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:sync	Grants permission to synchronize a restore point.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:create	Grants permission to create a vault.	write	vault *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • cbr:PolicyId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cbr:vaults:get	Grants permission to query a specified vault.	read	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:list	Grants permission to query the vault list.	list	vault *	-
			-	g:EnterpriseProjectId
cbr:vaults:update	Grants permission to modify a vault.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:delete	Grants permission to delete a vault.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:removeResources	Grants permission to dissociate resources.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:addResources	Grants permission to associate resources.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:setResources	Grants permission to set auto backup for a vault.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:associatePolicy	Grants permission to apply a policy to a vault.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:vaults:dissociatePolicy	Grants permission to remove a policy from a vault.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cbr:vaults:listExternalVaults	Grants permission to query the vault list in other regions.	list	vault *	-
cbr:vaults:migrateResources	Grants permission to migrate resources.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:backups:sync	Grants permission to synchronize a backup.	write	vault *	g:EnterpriseProjectId
cbr:backups:get	Grants permission to query a specified backup.	read	backup *	g:EnterpriseProjectId
cbr:backups:showMetadata	Grants permission to query backup metadata.	read	backup *	g:EnterpriseProjectId
cbr:backups:list	Grants permission to query all backups.	list	backup *	-
			-	g:EnterpriseProjectId
cbr:backups:delete	Grants permission to delete a backup.	write	backup *	g:EnterpriseProjectId
cbr:backups:replicate	Grants permission to replicate a backup.	write	backup *	g:EnterpriseProjectId
cbr:backups:restore	Grants permission to restore data from a backup.	write	backup *	g:EnterpriseProjectId
cbr:backups:update	Grants permission to update a backup.	write	backup *	g:EnterpriseProjectId
cbr:policies:list	Grants permission to query the policy list.	list	policy *	-
cbr:policies:create	Grants permission to create a policy.	write	policy *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	cbr:EnabledPolicy
cbr:policies:get	Grants permission to query a policy.	read	policy *	-
cbr:policies:update	Grants permission to modify a policy.	write	policy *	-
			-	cbr:EnabledPolicy
cbr:policies:delete	Grants permission to delete a policy.	write	policy *	-
cbr:vaults:listProtectables	Grants permission to query protectable resources.	list	-	g:EnterpriseProjectId
cbr:vaults:getProtectables	Grants permission to query a protectable resource.	read	-	-
cbr:backups:queryReplicationCapability	Grants permission to query the replication capability.	list	-	-
cbr:backups:checkAgent	Grants permission to query the Agent status.	read	-	-
cbr:vaults:listResourceInstances	Grants permission to query vault resources.	list	vault *	-
cbr:vaults:bulkCreateOrDeleteTags	Grants permission to batch add or delete tags of a vault resource.	write	vault *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cbr:vaults:setTags	Grants permission to add a tag to a vault resource.	write	vault *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cbr:vaults:deleteTags	Grants permission to delete a tag of a vault resource.	write	vault *	g:ResourceTag/<tag-key>
			-	g:TagKeys
cbr:vaults:getTags	Grants permission to query tags of a vault resource.	read	vault *	g:ResourceTag/<tag-key>
cbr:vaults:listProjectTags	Grants permission to query tags of a vault project.	list	vault *	-
cbr:backups:listStorageUsage	Grants permission to query capacity statistics.	list	-	-
cbr:vaults:updateOrder	Grants permission to update order information.	write	vault *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cbr:agents:addPath	Grants permission to add file paths.	write	agent *	-
cbr:agents:get	Grants permission to query a specified client.	read	agent *	-
cbr:agents:update	Grants permission to modify a client.	write	agent *	-
cbr:agents:register	Grants permission to register a client.	write	agent *	-
cbr:agents:delete	Grants permission to remove a client.	write	agent *	-
cbr:agents:removePath	Grants permission to remove file paths.	write	agent *	-
cbr:agents:list	Grants permission to query the client list.	list	agent *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cbr:backups:migratesCreate	Grants permission to migrate resources of a tenant.	write	-	-
cbr:backups:migratesIndex	Grants permission to query the migration results.	read	-	-
cbr:organizationPolicies:create	Grants permission to create an organizational policy.	write	-	-
cbr:organizationPolicies:listPolicyDetail	Grants permission to query organizational policy delivery info.	read	-	-
cbr:organizationPolicies:delete	Grants permission to delete an organizational policy.	write	-	-
cbr:organizationPolicies:update	Grants permission to modify an organizational policy.	write	-	-
cbr:organizationPolicies:list	Grants permission to query the organizational policy list.	list	-	-
cbr:organizationPolicies:get	Grants permission to query an organizational policy.	read	-	-

A CBR API usually supports one or more actions. **Table 5-28** lists actions supported by each API and dependencies of actions.

Table 5-28 Actions and dependencies supported by CBR APIs

API	Action	Dependencies
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	-
DELETE /v3/{project_id}/backups/{backup_id}/members/{member_id}	cbr:member:delete	-
GET /v3/{project_id}/checkpoints/{checkpoint_id}	cbr:vaults:showCheckpoint	-
GET /v3/{project_id}/vaults/summary	cbr:vaults:showSummary	-

API	Action	Dependencies
POST /v3/{project_id}/checkpoints/replicate	cbr:vaults:replicate	-
POST /v3/{project_id}/checkpoints	cbr:vaults:backup	• ecs:cloudServers:listServersDetails • evs:volumes:list
POST /v3/{project_id}/checkpoints/sync	cbr:vaults:sync	-
POST /v3/{project_id}/vaults	cbr:vaults:create	• ecs:cloudServers:listServersDetails • evs:volumes:list
POST /v3/{project_id}/vaults/order	cbr:vaults:create	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/vaults/{vault_id}	cbr:vaults:get	-
GET /v3/{project_id}/vaults	cbr:vaults:list	-
PUT /v3/{project_id}/vaults/{vault_id}	cbr:vaults:update	-
PUT /v3/{project_id}/vaults/batch-update	cbr:vaults:update	-
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	• ecs:cloudServers:listServersDetails • evs:volumes:list

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
POST /v3/{project_id}/backups/{backup_id}/restore	cbr:backups:restore	• ecs:cloudServers:listServersDetails • evs:volumes:list
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	• ecs:cloudServers:listServersDetails • evs:volumes:list
GET /v3/{project_id}/protectables/{protectable_type}/instances/{instance_id}	cbr:vaults:getProtectables	• ecs:cloudServers:listServersDetails • evs:volumes:list
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
GET /v3/{project_id}/agents	cbr:agents:list	-
POST /v3/migrates	cbr:backups:migratesCreate	-
GET /v3/migrates	cbr:backups:migratesIndex	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-29**, a resource URN must be specified in the SCP policy statements using that action, and the SCP policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (*) and the SCP policy applies to all resources. You can also set condition keys in an SCP policy to define resource types.

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

Table 5-29 Resource types supported by CBR

Resource Type	URN
Vault	cbr:<region>:<account-id>:vault:<vault-id>
Policy	cbr:<region>:<account-id>:policy:<policy-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

A Condition element lets you specify conditions for when an SCP 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, 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, cbr:) apply only to operations of the CBR service. For details, see **Table 5-30**.
  - 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 constitute a complete condition statement. An SCP policy applies only when its conditions are met. For supported condition operators, see condition operators.

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

Table 5-30 Service-specific condition keys supported by CBR

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
cbr:TargetOrgPaths	string	Single-valued	Organization path to which the target account specified in the API request for adding a share member of CBR belongs.
cbr:VaultId	string	Single-valued	Filters access based on the vault ID specified in the request parameter.
cbr:PolicyId	string	Single-valued	Filters access based on the policy ID specified in the request parameter.
cbr:EnabledPolicy	boolean	Single-valued	Whether to enable access filtering based on the policy.

5.10.2.2 Elastic Volume Service (EVS)

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 EVS, 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 EVS, see **Conditions**.

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

Table 5-31 Actions supported by EVS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
evs:volumes:create	Grants permission to create disks.	write	volume *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • evs:Encrypted • cbr:VaultId
evs:volumes:list	Grants permission to list disks.	list	-	g:EnterpriseProjectId
evs:volumes:get	Grants permission to query disks.	read	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:delete	Grants permission to delete disks.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:update	Grants permission to update disks.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:resize	Grants permission to expand disk capacities.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:modifyQos	Grants permission to modify disk QoS configurations.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:revert	Grants permission to recover disks from the recycle bin.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:recycle_policy:get	Grants permission to query the recycle bin policy.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
evs:recycle_policy:update	Grants permissions to update the recycle bin policy.	write	-	-
evs:volumes:changeChargeMode	Grants permission to change the billing mode of disks.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:snapshots:create	Grants permission to create snapshots for disks.	write	snapshot *	-
			volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:snapshots:list	Grants permission to list snapshots.	list	-	g:EnterpriseProjectId
evs:snapshots:get	Grants permission to query snapshots.	read	-	g:EnterpriseProjectId
evs:snapshots:delete	Grants permission to delete snapshots.	write	-	g:EnterpriseProjectId
evs:snapshots:update	Grants permission to update snapshots.	write	-	g:EnterpriseProjectId
evs:snapshots:rollback	Grants permissions to roll back data from snapshots.	write	-	g:EnterpriseProjectId
evs:types:get	Grants permission to query disk types.	read	-	-
evs:quotas:get	Grants permission to query EVS quotas.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
evs:volumes:tagResource	Grants permission to add tags to a disk.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
evs:volumes:unTagResource	Grants permission to delete tags from a disk.	write	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	g:TagKeys
evs:volumes:listTags	Grants permission to query all disk tags in a project.	list	-	-
evs:volumes:listTagsForResource	Grants permission to query disk tags.	read	volume *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
evs:volumes:listResourcesByTag	Grants permission to list disks by tag.	list	-	g:TagKeys
evs:volumes:use	Grants permission to allow ECSs and BMSs to use EVS disks.	write	-	g:EnterpriseProjectId

Each API of EVS usually supports one or more actions. **Table 5-32** lists the supported actions and dependencies.

Table 5-32 Actions and dependencies supported by EVS APIs

API	Action	Dependencies
POST /v2.1/{project_id}/cloudvolumes	evs:volumes:create	billing:order:pay

API	Action	Dependencies
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	-
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
POST /v5/{project_id}/volumes/batch-extend	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}/cloudvolumes/unsubscribe	evs:volumes:delete	billing:subscription:unsubscribe

API	Action	Dependencies
POST /v2/{project_id}/cloudvolumes/change-charge-mode	evs:volumes:changeChargeMode	• billing:order:pay • billing:subscription:renew
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	-
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	-

API	Action	Dependencies
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 SCP policy applies to. If you specify a resource type for any action in **Table 5-33**, 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 policy to define resource types.

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

Table 5-33 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

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, **evs:**) apply only to operations of the EVS service. For details, see **Table 5-34**.

- 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.

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

Table 5-34 Service-specific condition keys supported by EVS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
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 based on the disk type.
evs:VolumeSize	numeric	Single-valued	Filters access based on the disk capacity.
evs:VolumeIops	numeric	Single-valued	Filters access based on the disk IOPS.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
evs:VolumeThroughput	numeric	Single-valued	Filters access based on the disk throughput.
evs:ChargingMode	string	Single-valued	Filters access based on the disk billing mode.
evs:ServerServiceType	string	Single-valued	Filters access based on the service type of the cloud server.
evs:VolumeId	string	Single-valued	Filters access based on the disk ID.

5.10.2.3 Scalable File Service Turbo (SFS Turbo)

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 SFS Turbo, 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 SFS Turbo, see **Conditions**.

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

Table 5-35 Actions supported by SFS Turbo

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sfsturbo:shares:createShare	Grants permission to create SFS Turbo file systems.	write	shares *	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key> • sfsturbo:CryptKeyId • cbr:VaultId
sfsturbo:shares:deleteShare	Grants permission to delete SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAllShares	Grants permission to list SFS Turbo file systems.	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
sfsturbo:shares:getShare	Grants permission to query SFS Turbo file systems.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:extendShare	Grants permission to expand capacities of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sfsturbo:shares:updateHpcShare	Grants permission to update SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateShareSecurityGroup	Grants permission to change the security groups of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:addTag	Grants permission to add a tag to an SFS Turbo file system.	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
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 *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:batchResTag	Grants permission to batch add tags to an SFS Turbo file system.	tagging	shares *	• g:ResourceTag/<tag-key> • g:TagKeys
sfsturbo:shares:getAllTag	Grants permission to list all tags of an SFS Turbo file system.	list	-	g:EnterpriseProjectId
sfsturbo:shares:renameShare	Grants permission to change SFS Turbo file system names.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createDataRepositoryTask	Grants permission to create SFS Turbo backup vaults.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteDataRepositoryTask	Grants permission to delete SFS Turbo backup vaults.	write	shares *	• g:ResourceTag/<tag-key> g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sfsturbo:shares:getDataRepositoryTask	Grants permission to query SFS Turbo backup vaults.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:getAllDataRepositoryTasks	Grants permission to list SFS Turbo backup vaults.	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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	-	-
sfsturbo:shares:getFlavors	Grants permission to query the SFS Turbo file system types.	read	-	-
sfsturbo:shares:checkShareName	Grants permission to check SFS Turbo file system names.	read	-	-
sfsturbo:shares:showFsDir	Grants permission to query directories in SFS Turbo file systems.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteFsDir	Grants permission to delete directories from SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createFsDirQuota	Grants permission to configure limits for directories in SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsDirQuota	Grants permission to query limits of directories in SFS Turbo file systems.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sfsturbo:shares:deleteFsDirQuota	Grants permission to remove limits from directories in SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateFsDirQuota	Grants permission to update limits of directories in SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:batchCreateFsDirQuotas	Grants permission to batch configure limits for directories in SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listFsDirQuotas	Grants permission to list limits of directories in SFS Turbo file systems.	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:batchDeleteFsDirQuotas	Grants permission to batch delete limits of directories in SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:batchUpdateFsDirQuotas	Grants permission to batch update limits of directories in SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsDirUsage	Grants permission to query usages of directories in SFS Turbo file systems.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createFsAsyncTask	Grants permission to create asynchronous tasks of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showFsAsyncTask	Grants permission to query details of asynchronous tasks of SFS Turbo file systems.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sfsturbo:shares:listFsAsyncTasks	Grants permission to list asynchronous tasks of SFS Turbo file systems.	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteFsAsyncTask	Grants permission to delete asynchronous tasks of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createBackendTarget	Grants permission to add storage backends of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showBackendTargetInfo	Grants permission to query details about storage backends of SFS Turbo file systems.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:listBackendTargets	Grants permission to list storage backends of SFS Turbo file systems.	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deleteBackendTarget	Grants permission to remove storage backends of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateObsTargetPolicy	Grants permission to modify the auto synchronization policy between SFS Turbo file systems and OBS storage backends.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateObsTargetAttributes	Grants permission to modify storage backends of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sfsturbo:shares:listPermRules	Grants permission to list permission rules of SFS Turbo file systems.	list	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showPermRule	Grants permission to query details of permission rules of SFS Turbo file systems.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createPermRule	Grants permission to create permission rules of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updatePermRule	Grants permission to modify permission rules of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:deletePermRule	Grants permission to delete permission rules of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:showLdap	Grants permission to query the LDAP configuration of an SFS Turbo file system.	read	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:createLdap	Grants permission to create the LDAP configuration of an SFS Turbo file system.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
sfsturbo:shares:updateLdap	Grants permission to modify the LDAP configuration of SFS Turbo file systems.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sfsturbo:shares:deleteLdap	Grants permission to delete the LDAP configuration of an SFS Turbo file system.	write	shares *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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 5-36** lists the supported actions and dependencies.

Table 5-36 Actions and dependencies supported by SFS Turbo APIs

API	Action	Dependencies
POST /v1/{project_id}/sfs-turbo/shares	sfsturbo:shares:createShare	• billing:order:pay • billing:contract:viewDiscount • vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get • vpc:securityGroups:create • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:securityGroupRules:get • vpc:securityGroupRules:create • vpc:quotas:list • cbr:backups:get • cbr:vaults:addResources • evs:types:get • kms:cmk:listGrants • kms:cmk:createGrant • kms:cmk:get • sfsturbo:shares:getAZInfo • sfsturbo:shares:getQuota • sfsturbo:shares:getFlavors • sfsturbo:shares:checkShareName • eps:enterpriseProjects:list
GET /v1/{project_id}/sfs-turbo/shares/detail	sfsturbo:shares:getAllShares	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:getShare	-

API	Action	Dependencies
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}	sfsturbo:shares:deleteShare	• vpc:ports:get • vpc:ports:delete • vpc:securityGroupRules:delete • vpc:securityGroups:delete
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:extendShare	• billing:order:pay • vpc:vpcs:get • vpc:subnets:get • vpc:ports:get • vpc:ports:create • vpc:ports:update
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/action	sfsturbo:shares:updateShareSecurityGroup	• vpc:ports:update • vpc:securityGroups:get • vpc:securityGroupRules:create • vpc:securityGroupRules:delete
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	-
GET /v1/{project_id}/sfs-turbo/tags	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	• obs:bucket:putBucketPolicy • vpc:ports:get • vpc:ports:create • vpc:subnets:get
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	-
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	-

API	Action	Dependencies
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	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/dir-usage	sfsturbo:shares:showFsDirUsage	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules	sfsturbo:shares:createPermRule	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules	sfsturbo:shares:listPermRules	-
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:showPermRule	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:updatePermRule	-
DELETE /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/perm-rules/{rule_id}	sfsturbo:shares:deletePermRule	-
POST /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:createLdap	-

API	Action	Dependencies
GET /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:showLdap	-
PUT /v1/{project_id}/sfs-turbo/shares/{share_id}/fs/ldap	sfsturbo:shares:updateLdap	-
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	-
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	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-37**, 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 policy to define resource types.

The following table lists the resource types that you can specify in SCP statements for SFS Turbo.

Table 5-37 Resource types supported by SFS Turbo

Resource Type	URN	Condition Key
shares	shares *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Conditions

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, **sfsturbo:**) only apply to operations of the SFS Turbo service. For details, see **Table 5-38**.
  - 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.

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

Table 5-38 Service-specific condition keys supported by SFS Turbo

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

5.10.3 Networking

5.10.3.1 Virtual Private Cloud (VPC)

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 permission to that member account or OU. Instead, the SCPs 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 VPC, 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 VPC, see **Conditions**.

The following table lists the actions that you can define in SCP statements for VPC.

Table 5-39 Actions supported by VPC

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:vpcs:create	Grants permission to create a VPC.	write	vpc *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
vpc:vpcs:get	Grants permission to query VPC details.	read	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:vpcs:list	Grants permission to query VPCs.	list	vpc *	-
			-	g:EnterpriseProjectId
vpc:vpcs:update	Grants permission to modify a VPC.	write	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:vpcs:delete	Grants permission to delete a VPC.	write	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:subnets:create	Grants permission to create a subnet.	write	subnet *	-
			vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:subnets:get	Grants permission to query subnet details.	read	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:subnets:list	Grants permission to query subnets.	list	subnet *	-
			-	g:EnterpriseProjectId
vpc:subnets:update	Grants permission to modify a subnet.	write	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:subnets:delete	Grants permission to delete a subnet.	write	subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:quotas:list	Grants permission to query quotas.	list	-	-
vpc:privateIps:create	Grants permission to assign a private IP address.	write	privateIp *	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId
vpc:privateIps:get	Grants permission to query the details of a private IP address.	read	privateIp *	• vpc:PrivateIpId • vpc:SubnetId
vpc:privateIps:list	Grants permission to query private IP addresses.	list	privateIp *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:privateIps:delete	Grants permission to release a private IP address.	write	privateIp *	• vpc:PrivateIpId • vpc:SubnetId
vpc:securityGroups:create	Grants permission to create a security group.	write	security Group *	-
			-	g:EnterpriseProjectId
vpc:securityGroups:get	Grants permission to query the details of a security group.	read	security Group *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroups:list	Grants permission to query security groups.	list	security Group *	-
			-	g:EnterpriseProjectId
vpc:securityGroups:update	Grants permission to modify a security group.	write	security Group *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroups:delete	Grants permission to delete a security group.	write	security Group *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:create	Grants permission to create a security group rule.	write	securityGroupRule *	-
			security Group *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:get	Grants permission to query the details of a security group rule.	read	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:list	Grants permission to query security group rules.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:securityGroupRules:update	Grants permission to modify a security group rule.	write	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:securityGroupRules:delete	Grants permission to delete a security group rule.	write	securityGroupRule *	• g:EnterpriseProjectId • vpc:SecurityGroupId
vpc:ports:create	Grants permission to create a port.	write	port *	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:ports:get	Grants permission to query port details.	read	port *	• vpc:SubnetId • vpc:PortId • g:EnterpriseProjectId
vpc:ports:list	Grants permission to query ports.	list	port *	-
			-	g:EnterpriseProjectId
vpc:ports:update	Grants permission to modify a port.	write	port *	• vpc:SubnetId • vpc:PortId • g:EnterpriseProjectId
vpc:ports:delete	Grants permission to delete a port.	write	port *	• vpc:SubnetId • vpc:PortId • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:peerings:create	Grants permission to create a VPC peering connection.	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:AccepterVpcOrgPath • vpc:AccepterVpcOwner
			vpc *	• g:ResourceTag/<tag-key> • vpc:VpcId
vpc:peerings:get	Grants permission to query the details of a VPC peering connection.	read	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId
vpc:peerings:list	Grants permission to query VPC peering connections.	list	peering *	-
vpc:peerings:accept	Grants permission to accept a VPC peering connection.	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId • vpc:RequesterVpcOrgPath • vpc:RequesterVpcOwner
vpc:peerings:reject	Grants permission to reject a VPC peering connection.	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:peerings:update	Grants permission to modify a VPC peering connection.	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId
vpc:peerings:delete	Grants permission to delete a VPC peering connection.	write	peering *	• vpc:AccepterVpcId • vpc:RequesterVpcId • vpc:PeeringId
vpc:routeTables:create	Grants permission to create a route table.	write	routeTable *	-
			vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
vpc:routeTables:get	Grants permission to query route table details.	read	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId
vpc:routeTables:list	Grants permission to query route tables.	list	routeTable *	-
			-	g:EnterpriseProjectId
vpc:routeTables:update	Grants permission to modify a route table.	write	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId
vpc:routeTables:associate	Grants permission to associate a route table.	write	routeTable *	• vpc:RouteTableId • vpc:VpcId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:routeTables:delete	Grants permission to delete a route table.	write	routeTable *	• vpc:RouteTableId • vpc:VpcId • g:EnterpriseProjectId
vpc:flowLogs:create	Grants permission to create a VPC flow log.	write	flowLog *	-
			port	vpc:PortId
			subnet	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId
			vpc	• g:ResourceTag/<tag-key> • vpc:VpcId
vpc:flowLogs:get	Grants permission to query VPC flow logs or their details.	read	flowLog *	vpc:FlowLogId
vpc:flowLogs:list	Grants permission to query VPC flow logs.	read	flowLog *	-
vpc:flowLogs:update	Grants permission to modify a VPC flow log.	write	flowLog *	vpc:FlowLogId
vpc:flowLogs:delete	Grants permission to delete a VPC flow log.	write	flowLog *	vpc:FlowLogId
vpc:addressGroups:create	Grants permission to create an IP address group.	write	addressGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
vpc:addressGroups:get	Grants permission to query the details of an IP address group.	read	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId
vpc:addressGroups:list	Grants permission to query IP address groups.	list	addressGroup *	-
			-	g:EnterpriseProjectId
vpc:addressGroups:update	Grants permission to modify an IP address group.	write	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId
vpc:addressGroups:delete	Grants permission to delete an IP address group.	write	addressGroup *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:AddressGroupId
vpc:firewalls:create	Grants permission to create a network ACL.	write	firewall *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:firewalls:get	Grants permission to query the details of a network ACL.	read	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId
vpc:firewalls:list	Grants permission to query network ACLs.	list	firewall *	-
			-	g:EnterpriseProjectId
vpc:firewalls:update	Grants permission to modify a network ACL.	write	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId • vpc:FirewallRuleDirection • vpc:FirewallRuleProtocol • vpc:FirewallRuleAction • vpc:FirewallRuleSourcePort • vpc:FirewallRuleDestinationPort • vpc:FirewallOperationType
			subnet	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId • g:EnterpriseProjectId
vpc:firewalls:delete	Grants permission to delete a network ACL.	write	firewall *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:FirewallId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:vpcs:createTags	Grants permission to add tags to a VPC.	tagging	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
			-	• g:RequestTag/<tag-key> • g:TagKeys
vpc:vpcs:listTags	Grants permission to query VPC tags.	read	vpc *	-
vpc:vpcs:deleteTags	Grants permission to delete tags from a VPC.	tagging	vpc *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId
			-	g:TagKeys
vpc:subnets:createTags	Grants permission to add tags to a subnet.	tagging	subnet *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId • vpc:SubnetId
			-	• g:RequestTag/<tag-key> • g:TagKeys
vpc:subnets:listTags	Grants permission to query subnet tags.	read	subnet *	-
vpc:subnets:deleteTags	Grants permission to delete tags from a subnet.	tagging	subnet *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • vpc:VpcId • vpc:SubnetId
			-	g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:subNetworkInterfaces:create	Grants permission to create supplementary network interfaces.	write	subNetworkInterface *	-
			subnet *	• g:ResourceTag/<tag-key> • vpc:SubnetId • vpc:VpcId
vpc:subNetworkInterfaces:get	Grants permission to query the details of a supplementary network interface.	read	subNetworkInterface *	• vpc:SubnetId • vpc:SubNetworkInterfaceId
vpc:subNetworkInterfaces:list	Grants permission to query supplementary network interfaces.	list	subNetworkInterface *	-
vpc:subNetworkInterfaces:update	Grants permission to modify a supplementary network interface.	write	subNetworkInterface *	• vpc:SubnetId • vpc:SubNetworkInterfaceId
vpc:subNetworkInterfaces:delete	Grants permission to delete a supplementary network interface.	write	subNetworkInterface *	• vpc:SubnetId • vpc:SubNetworkInterfaceId
vpc:networks:create	Grants permission to create a network.	write	network *	-
vpc:networks:get	Grants permission to query network details.	read	network *	-
vpc:networks:list	Grants permission to query networks.	list	network *	-
vpc:networks:update	Grants permission to update a network.	write	network *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
vpc:networks:delete	Grants permission to delete a network.	write	addressGroup *	-

Each API of VPC usually supports one or more actions. **Table 5-40** lists the supported actions and dependencies.

Table 5-40 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	-
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	-

API	Action	Dependencies
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	-
DELETE /v1/{project_id}/security-groups/{security_group_id}	vpc:securityGroups:delete	-
POST /v1/{project_id}/security-group-rules	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	-
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	-

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

API	Action	Dependencies
GET /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:get	-
GET /v3/{project_id}/vpc/address-groups	vpc:addressGroups:list	-
PUT /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:update	-
DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}	vpc:addressGroups:delete	-
DELETE /v3/{project_id}/vpc/address-groups/{address_group_id}/force	vpc:addressGroups:delete	-
POST /v2.0/{project_id}/vpcs/{vpc_id}/tags/action	vpc:vpcs:createTags	-
POST 01 /v2.0/{project_id}/vpcs/{vpc_id}/tags/action	vpc:vpcs:deleteTags	-
POST /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcs:createTags	-
POST /v2.0/{project_id}/vpcs/resource_instances/action	vpc:vpcs:listTags	-
GET /v2.0/{project_id}/vpcs/tags	vpc:vpcs:listTags	-
GET /v2.0/{project_id}/vpcs/{vpc_id}/tags	vpc:vpcs:listTags	-
DELETE /v2.0/{project_id}/vpcs/{vpc_id}/tags/{key}	vpc:vpcs:deleteTags	-
POST 01 /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnets:creatTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags/action	vpc:subnets:deleteTags	-
POST /v2.0/{project_id}/subnets/{subnet_id}/tags	vpc:subnets:creatTags	-
POST /v2.0/{project_id}/subnets/resource_instances/action	vpc:subnets:listTags	-

API	Action	Dependencies
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	-
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/migrate	vpc:subNetworkInterfaces:update	-
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	-

Resources

A resource type indicates the resources that an SCP is applied. If you specify a resource type for any action in **Table 5-41**, a resource URN must be specified in the SCP policy statements using that action, and the SCP policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (*) and the SCP 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 VPC.

Table 5-41 Resource types supported by VPC

Resource Type	URN
vpc	vpc:<region>:<account-id>:vpc:<vpc-id>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
privateIp	vpc:<region>:<account-id>:privateIp:<private-ip-id>
securityGroup	vpc:<region>:<account-id>:securityGroup:<security-group-id>
securityGroupRule	vpc:<region>:<account-id>:securityGroupRule:<security-group-rule-id>
port	vpc:<region>:<account-id>:port:<port-id>
peering	vpc:<region>:<account-id>:peering:<peering-id>
routeTable	vpc:<region>:<account-id>:routeTable:<route-table-id>
flowLog	vpc:<region>:<account-id>:flowLog:<flow-log-id>
addressGroup	vpc:<region>:<account-id>:addressGroup:<address-group-id>
firewall	vpc:<region>:<account-id>:firewall:<firewall-id>
publicip	vpc:<region>:<account-id>:publicip:<publicip-id>
bandwidth	vpc:<region>:<account-id>:bandwidth:<bandwidth-id>
network	vpc:<region>:<account-id>:network:<network-id>

Conditions

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, **vpc:**) apply only to operations on VPC. For details, see **Table 5-42**.
  - 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.

The following table lists the condition keys that you can define in SCPs for VPC. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-42 Service-specific condition keys supported by VPC

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
vpc:VpcId	string	Multivalued	Filters accesses by VPC ID.
vpc:SubnetId	string	Multivalued	Filters accesses by subnet ID.
vpc:SecurityGroupId	string	Multivalued	Filters accesses by security group ID.
vpc:PeeringId	string	Multivalued	Filters accesses by peering connection ID.
vpc:AccepterVpcId	string	Multivalued	Filters accesses by the ID of the VPC owned by the specified recipient.
vpc:AccepterVpcOrgPath	string	Multivalued	Filters accesses by the organization path of the specified recipient of the VPC peering connection.
vpc:AccepterVpcOwner	string	Multivalued	Filters accesses by the account ID of the specified recipient of the VPC peering connection.
vpc:RequesterVpcOrg-Path	string	Multivalued	Filters accesses by the organization path of the specified requester of the VPC peering connection.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
vpc:RequesterVpcOwner	string	Multivalued	Filters accesses by the account ID of the specified requester of the VPC peering connection.
vpc:RequesterVpcId	string	Multivalued	Filters accesses by the ID of the VPC owned by the specified requester.
vpc:RouteTableId	string	Multivalued	Filters accesses by route table ID.
vpc:FlowLogId	string	Multivalued	Filters accesses by flow log ID.
vpc:AddressGroupId	string	Multivalued	Filters accesses by IP address group ID.
vpc:FirewallId	string	Multivalued	Filters accesses by network ACL ID.
vpc:PrivateIpId	string	Multivalued	Filters accesses by private IP address ID.
vpc:PortId	string	Multivalued	Filters accesses by port ID.
vpc:FirewallRuleDirection	string	Multivalued	Filters accesses by network ACL rule. The value can be **ingress** or **egress**.
vpc:FirewallRuleProtocol	string	Multivalued	Filters accesses by network ACL protocol. The value can be **TCP**, **UDP**, **ICMP**, **ICMPv6**, or **Any**.
vpc:FirewallRuleAction	string	Multivalued	Filters accesses by network ACL policy. The value can be **Allow** or **Deny**.
vpc:FirewallRuleSourcePort	numeric	Multivalued	Filters accesses by source port specified in the network ACL rule.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
vpc:FirewallRuleDestinationPort	numeric	Multivalued	Filters accesses by destination port specified in the network ACL rule.
vpc:FirewallOperationType	string	Multivalued	Filters accesses by network ACL operation type. The value can be **updateAcl**, **associateSubnet**, **disassociateSubnet**, **insertRule**, **updateRule**, or **removeRule**.

5.10.3.2 Elastic IP (EIP)

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 permission to that member account or OU. Instead, the SCPs 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 EIP, 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 EIP, see **Conditions**.

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

Table 5-43 Actions supported by EIP

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
eip:publicIps:create	Grants permission to assign an EIP.	write	publicip *	-
			-	g:EnterpriseProjectId
eip:publicIps:batchCreate	Grants permission to assign EIPs in batches.	write	publicip *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
eip:publicIps:list	Grants permission to query EIPs.	list	publicip *	-
			-	g:EnterpriseProjectId
eip:publicIps:count	Grants permission to query the number of EIPs.	list	publicip *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
eip:publicIps:get	Grants permission to query a specific EIP.	read	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:publicIps:update	Grants permission to modify an EIP.	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:enableNat64	Grants permission to enable NAT64 for an EIP.	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:disableNat64	Grants permission to enable NAT64 for an EIP.	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:associateInstance	Grants permission to bind an EIP to a network interface.	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:disassociateInstance	Grants permission to unbind an EIP from a network interface.	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:attachBandwidth	Grants permission to associate an EIP with a bandwidth.	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:detachBandwidth	Grants permission to remove an EIP from a shared bandwidth.	write	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
			bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:publicIps:delete	Grants permission to release an EIP.	write	publicip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:publicIps:createTags	Grants permission to add tags to an EIP.	tagging	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
eip:publicIps:listTags	Grants permission to query tags of an EIP.	list	publicip *	-
eip:publicIps:deleteTags	Grants permission to delete tags from an EIP.	tagging	publicip *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
eip:bandwidths:insertPublicIps	Grants permission to add EIPs to a shared bandwidth.	write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:bandwidths:removePublicIps	Grants permission to remove EIPs from a shared bandwidth.	write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:bandwidths:create	Grants permission to create a shared bandwidth.	write	bandwidth *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
eip:bandwidths:batchCreate	Grants permission to create shared bandwidths in batches.	write	bandwidth *	-
eip:bandwidths:list	Grants permission to query bandwidths.	list	bandwidth *	-
			-	g:EnterpriseProjectId
eip:bandwidths:update	Grants permission to modify a bandwidth.	write	bandwidth *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
eip:bandwidths:get	Grants permission to query a bandwidth.	read	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:bandwidths:delete	Grants permission to delete a shared bandwidth.	write	bandwidth *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
eip:bandwidthPkgs:list	Grants permission to query bandwidth add-on packages.	list	bandwidthPkg *	-
eip:publicipPools:get	Grants permission to query an EIP pool.	read	publicipPool *	-

Each API of EIP usually supports one or more actions. **Table 5-44** lists the supported actions and dependencies.

Table 5-44 Actions and dependencies supported by EIP APIs

API	Action	Dependencies
POST /v2.0/{project_id}/publicips	eip:publicIps:create	-

API	Action	Dependencies
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 /v2/{project_id}/elasticips	eip:publicIps:count	-
GET /v2/{project_id}/publicip/instances	eip:publicIps:count	-
GET /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:get	-
PUT /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:update	-
POST /v2.0/{project_id}/publicips/change-to-period	eip:publicIps:update	bss:renewal:update
PATCH /v2/{project_id}/batchpublicips	eip:publicIps:disassociateInstance	-
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	-
DELETE /v1/{project_id}/publicips/{publicip_id}	eip:publicIps:delete	-

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

API	Action	Dependencies
PUT /v2.0/{project_id}/bandwidths/{bandwidth_id}	eip:bandwidths:update	-
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	-
GET /v3/{project_id}/eip/publicip-pools/{publicip_pool_id}	eip:publicipPools:get	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/enable-nat64	eip:publicIps:enableNat64	-
POST /v3/{project_id}/eip/publicips/{publicip_id}/disable-nat64	eip:publicIps:disableNat64	-

Resources

A resource type indicates the resources that an SCP is applied. If you specify a resource type for any action in **Table 5-45**, a resource URN must be specified in the SCP policy statements using that action, and the SCP policy applies only to the resource. If no resource type is specified, the Resource element is marked with an asterisk (*) and the SCP 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 an SCP for EIP.

Table 5-45 Resource types supported by EIP

Resource Type	URN
bandwidthPkg	eip:<region>:<account-id>:bandwidthPkg:<bandwidthPkg-id>
publicipPool	eip:<region>:<account-id>:publicipPool:<publicipPool-id>
publicip	eip:<region>:<account-id>:publicip:<publicip-id>
bandwidth	eip:<region>:<account-id>:bandwidth:<bandwidth-id>

Conditions

EIP 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.

5.10.3.3 NAT Gateway

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 NAT Gateway, 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 NAT Gateway, see **Conditions**.

The following table lists the actions that you can define in SCP statements for NAT Gateway.

Table 5-46 Actions supported by NAT Gateway

Action	Description	Access Level	Resource Type (*: required)	Condition Key
nat:privateNatGateways:list	Grants permission to query private NAT gateways.	list	privateGateway *	g:EnterpriseProjectId
nat:privateNatGateways:create	Grants permission to create a private NAT gateway.	write	privateGateway *	-
			subnet *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatGateways:delete	Grants permission to delete a private NAT gateway.	write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatGateways:get	Grants permission to query a private NAT gateway.	read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatGateways:update	Grants permission to update a private NAT gateway.	write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatDnatRules:list	Grants permission to query DNAT rules on a private NAT gateway.	list	privateDnatRule *	g:EnterpriseProjectId
nat:privateNatDnatRules:create	Grants permission to create a DNAT rule on a private NAT gateway.	write	privateGateway *	g:ResourceTag/<tag-key>
			privateDnatRule *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			privateTransitIp *	g:ResourceTag/<tag-key>
			port	-
			-	g:EnterpriseProjectId
nat:privateNatDnatRules:delete	Grants permission to delete a DNAT rule on a private NAT gateway.	write	private Gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			private DnatRule *	g:EnterpriseProjectId
nat:privateNatDnatRules:get	Grants permission to query a DNAT rule on a private NAT gateway.	read	private Gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			private DnatRule *	g:EnterpriseProjectId
nat:privateNatDnatRules:update	Grants permission to update a DNAT rule on a private NAT gateway.	write	private Gateway *	g:ResourceTag/<tag-key>
			private DnatRule *	-
			privateTransitIp	g:ResourceTag/<tag-key>
			port	-
			-	g:EnterpriseProjectId
nat:privateNatSnatRules:list	Grants permission to query SNAT rules on a private NAT gateway.	list	privateSnatRule *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
nat:privateNatSnatRules:create	Grants permission to create an SNAT rule on a private NAT gateway.	write	privateGateway *	g:ResourceTag/<tag-key>
			privateSnatRule *	-
			privateTransitIp *	g:ResourceTag/<tag-key>
			subnet	-
			-	g:EnterpriseProjectId
nat:privateNatSnatRules:delete	Grants permission to delete an SNAT rule on a private NAT gateway.	write	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			privateSnatRule *	g:EnterpriseProjectId
nat:privateNatSnatRules:get	Grants permission to query an SNAT rule on a private NAT gateway.	read	privateGateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			privateSnatRule *	g:EnterpriseProjectId
nat:privateNatSnatRules:update	Grants permission to update an SNAT rule on a private NAT gateway.	write	privateGateway *	g:ResourceTag/<tag-key>
			privateSnatRule *	-
			privateTransitIp	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
nat:privateNatTransitIps:list	Grants permission to query transit IP addresses.	list	privateTransitIp *	g:EnterpriseProjectId
nat:privateNatTransitIps:create	Grants permission to assign a transit IP address.	write	privateTransitIp *	-
			subnet	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatTransitIps:delete	Grants permission to release a transit IP address.	write	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:privateNatTransitIps:get	Grants permission to query a transit IP address.	read	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:natGateways:list	Grants permission to query public NAT gateways.	list	gateway *	g:EnterpriseProjectId
nat:natGateways:create	Grants permission to create a public NAT gateway.	write	gateway *	-
			vpc *	-
			subnet *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
nat:natGateways:delete	Grants permission to delete a public NAT gateway.	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
nat:natGateways:get	Grants permission to query a public NAT gateway.	read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:natGateways:update	Grants permission to update a public NAT gateway.	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
nat:dnatRules:list	Grants permission to query DNAT rules on a public NAT gateway.	list	dnatRule *	g:EnterpriseProjectId
nat:dnatRules:create	Grants permission to create a DNAT rule on a public NAT gateway.	write	gateway *	g:ResourceTag/<tag-key>
			dnatRule *	-
			publicip	-
			globalEip	-
			port	-
			-	g:EnterpriseProjectId
nat:dnatRules:get	Grants permission to query a DNAT rule on a public NAT gateway.	read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			dnatRule *	g:EnterpriseProjectId
nat:dnatRules:update	Grants permission to update a DNAT rule on a public NAT gateway.	write	gateway *	g:ResourceTag/<tag-key>
			dnatRule *	-
			publicip	-
			globalEip	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			port	-
			-	g:EnterpriseProjectId
nat:dnatRules:delete	Grants permission to delete a DNAT rule on a public NAT gateway.	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			dnatRule *	g:EnterpriseProjectId
nat:snatRules:list	Grants permission to query SNAT rules on a public NAT gateway.	list	snatRule *	g:EnterpriseProjectId
nat:snatRules:create	Grants permission to create an SNAT rule on a public NAT gateway.	write	gateway *	g:ResourceTag/<tag-key>
			snatRule *	-
			publicip	-
			globalEip	-
			subnet	-
			-	g:EnterpriseProjectId
nat:snatRules:get	Grants permission to query an SNAT rule on a public NAT gateway.	read	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			snatRule *	g:EnterpriseProjectId
nat:snatRules:update	Grants permission to update an SNAT rule on a public NAT gateway.	write	gateway *	g:ResourceTag/<tag-key>
			snatRule *	-
			publicip	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			globalEip	-
			-	g:EnterpriseProjectId
nat:snatRules:delete	Grants permission to delete an SNAT rule on a public NAT gateway.	write	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			snatRule *	g:EnterpriseProjectId
nat:privateNatGateways:createTags	Grants permission to add a tag to a private NAT gateway.	tagging	privateGateway *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatGateways:deleteTags	Grants permission to delete a tag of a private NAT gateway.	tagging	privateGateway *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatGateways:listTags	Grants permission to query tags of a private NAT gateway.	list	privateGateway	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
nat:privateNatTransitIps:createTags	Grants permission to add a tag to a transit IP address.	tagging	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
nat:privateNatTransitIps:deleteTags	Grants permission to delete a tag of a transit IP address.	tagging	privateTransitIp *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:privateNatTransitIps:listTags	Grants permission to query tags of a transit IP address.	list	privateTransitIp	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
nat:natGateways:createTags	Grants permission to add a tag to a public NAT gateway.	tagging	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:natGateways:deleteTags	Grants permission to delete a tag of a public NAT gateway.	tagging	gateway *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
nat:natGateways:listTags	Grants permission to query tags of a public NAT gateway.	list	gateway	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Each API of NAT Gateway usually supports one or more actions. **Table 5-47** lists the supported actions and dependencies.

Table 5-47 Actions and dependencies supported by NAT Gateway 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	-
GET /v2/{project_id}/nat_gateways	nat:natGateways:list	-
POST /v2/{project_id}/nat_gateways	nat:natGateways:create	-
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:delete	-
GET /v2/{project_id}/nat_gateways/{nat_gateway_id}	nat:natGateways:get	-

API	Action	Dependencies
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	• eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
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
GET /v2/{project_id}/snat_rules/{snat_rule_id}	nat:snatRules:get	-
PUT /v2/{project_id}/snat_rules/{snat_rule_id}	nat:snatRules:update	• eip:publicIps:associateInstance • eip:publicIps:disassociateInstance

API	Action	Dependencies
DELETE /v2/{project_id}/nat_gateways/{nat_gateway_id}/snat_rules/{snat_rule_id}	nat:snatRules:delete	eip:publicIps:disassociateInstance
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	-
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

API	Action	Dependencies
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 /v2.0/{project_id}/nat_gateways/resource_instances/action	nat:natGateways:listTags	-
POST /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags/action	nat:natGateways:createTags	nat:natGateways:deleteTags
POST /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags	nat:natGateways:createTags	-
GET /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags	nat:natGateways:listTags	-
DELETE /v2.0/{project_id}/nat_gateways/{nat_gateway_id}/tags/{key}	nat:natGateways:deleteTags	-
GET /v2.0/{project_id}/nat_gateways/tags	nat:natGateways:listTags	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-48**, 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 NAT Gateway.

Table 5-48 Resource types supported by NAT Gateway

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>

Conditions

Only global condition keys applicable to all cloud services can be configured for NAT Gateway. For details, see Global Condition Keys.

5.10.3.4 Elastic Load Balance (ELB)

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 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 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 ELB, see **Conditions**.

The following table lists the actions that you can define in SCP statements for ELB.

Table 5-49 Actions supported by ELB

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:flavors:show	Grants permission to query a given flavor.	read	flavor *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:flavors:list	Grants permission to query flavors.	list	flavor *	-
elb:quotas:list	Grants permission to query quotas.	list	-	-
elb:quotas:show	Grants permission to query the maximum number of resources of a specified type that can be created.	read	-	-
elb:availability-zones:list	Grants permission to query AZs.	list	availabilityZone *	-
			-	g:EnterpriseProjectId
elb:loadbalancers:list	Grants permission to query load balancers.	list	loadbalancer *	-
			-	g:EnterpriseProjectId
elb:loadbalancers:show	Grants permission to query the details of a load balancer.	read	loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:loadbalancers:create	Grants permission to create a load balancer.	write	loadbalancer *	-
			subnet	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • elb:AssociatePublicips
elb:loadbalancers:update	Grants permission to modify a load balancer.	write	subnet	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
			loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • elb:AssociatePublicips
elb:loadbalancers:delete	Grants permission to delete a load balancer.	write	loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:listeners:create	Grants permission to add a listener.	write	listener *	g:EnterpriseProjectId
			loadbalancer *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
elb:listeners:update	Grants permission to modify a listener.	write	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:listeners:list	Grants permission to query listeners.	list	listener *	-
			-	g:EnterpriseProjectId
elb:listeners:show	Grants permission to query the details of a listener.	read	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
elb:listeners:delete	Grants permission to delete a listener.	write	listener *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:certificates:list	Grants permission to query certificates.	list	certificate *	-
			-	g:EnterpriseProjectId
elb:certificates:show	Grants permission to query the details of a certificate.	read	certificate *	-
elb:certificates:create	Grants permission to add a certificate.	write	certificate *	-
			-	g:EnterpriseProjectId
elb:certificates:update	Grants permission to modify a certificate.	write	certificate *	-
elb:certificates:delete	Grants permission to delete a certificate.	write	certificate *	-
elb:certificates:setPrivateKeyEcho	Grants permission to enable or disable the private key feature.	write	-	-
elb:certificates:getPrivateKeyEcho	Grants permission to query whether the private key feature is enabled.	write	-	-
elb:agreements:list	Grants permission to query signing records.	list	agreement *	-
elb:agreements:show	Grants permission to obtain signing information details.	read	agreement *	-
elb:agreements:create	Grants permission to create signing records.	write	agreement *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:agreements:update	Grants permission to modify signing records.	write	agreement *	-
elb:healthmonitors:create	Grants permission to configure a health check.	write	healthmonitor *	g:EnterpriseProjectId
			pool *	g:EnterpriseProjectId
elb:healthmonitors:update	Grants permission to modify a health check.	write	healthmonitor *	g:EnterpriseProjectId
elb:healthmonitors:delete	Grants permission to delete a health check.	write	healthmonitor *	g:EnterpriseProjectId
elb:healthmonitors:show	Grants permission to query health check details.	read	healthmonitor *	g:EnterpriseProjectId
elb:healthmonitors:list	Grants permission to query health checks.	list	healthmonitor *	-
			-	g:EnterpriseProjectId
elb:ipgroups:list	Grants permission to query IP address groups.	list	ipgroup *	-
			-	g:EnterpriseProjectId
elb:ipgroups:show	Grants permission to query the details of an IP address group.	read	ipgroup *	-
elb:ipgroups:create	Grants permission to create an IP address group.	write	ipgroup *	-
			-	g:EnterpriseProjectId
elb:ipgroups:update	Grants permission to modify an IP address group.	write	ipgroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:ipgroups:delete	Grants permission to delete an IP address group.	write	ipgroup *	-
elb:l7policies:create	Grants permission to add a forwarding policy to HTTP or HTTPS listeners.	write	listener *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			l7policy *	g:EnterpriseProjectId
			pool	g:EnterpriseProjectId
elb:l7policies:update	Grants permission to modify a forwarding policy.	write	l7policy *	g:EnterpriseProjectId
			listener	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			pool	g:EnterpriseProjectId
elb:l7policies:delete	Grants permission to delete a forwarding policy.	write	l7policy *	g:EnterpriseProjectId
elb:l7policies:show	Grants permission to query the details of a forwarding policy.	read	l7policy *	g:EnterpriseProjectId
elb:l7policies:list	Grants permission to query forwarding policies.	list	l7policy *	-
			-	g:EnterpriseProjectId
elb:l7rules:create	Grants permission to add a forwarding rule.	write	l7rule *	g:EnterpriseProjectId
			l7policy *	g:EnterpriseProjectId
elb:l7rules:update	Grants permission to modify a forwarding rule.	write	l7rule *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:l7rules:list	Grants permission to query forwarding rules.	list	l7policy *	-
			l7rule *	-
			-	g:EnterpriseProjectId
elb:l7rules:show	Grants permission to query the details of a forwarding rule.	read	l7rule *	g:EnterpriseProjectId
elb:l7rules:delete	Grants permission to delete a forwarding rule.	write	l7rule *	g:EnterpriseProjectId
elb:logtanks:list	Grants permission to query logs.	list	logtank *	-
			-	g:EnterpriseProjectId
elb:logtanks:show	Grants permission to query the details of a log.	read	logtank *	g:EnterpriseProjectId
elb:logtanks:create	Grants permission to create a log.	write	logtank *	g:EnterpriseProjectId
			loadbalancer *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
elb:logtanks:update	Grants permission to modify a log.	write	logtank *	g:EnterpriseProjectId
elb:logtanks:delete	Grants permission to delete a log.	write	logtank *	g:EnterpriseProjectId
elb:pools:list	Grants permission to query backend server groups.	list	pool *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:pools:show	Grants permission to query the details of a backend server group.	read	pool *	g:EnterpriseProjectId
elb:pools:create	Grants permission to create a backend server group.	write	loadbalancer	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			listener	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			pool *	g:EnterpriseProjectId
elb:pools:update	Grants permission to modify a backend server group.	write	pool *	g:EnterpriseProjectId
elb:pools:delete	Grants permission to delete a backend server group.	write	pool *	g:EnterpriseProjectId
elb:members:list	Grants permission to query backend servers.	list	pool	-
			member *	-
			-	g:EnterpriseProjectId
elb:members:show	Grants permission to query the details of a backend server.	read	member *	g:EnterpriseProjectId
elb:members:create	Grants permission to add a backend server.	write	member *	g:EnterpriseProjectId
			pool *	g:EnterpriseProjectId
			subnet	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
elb:members:update	Grants permission to modify the configurations of a backend server.	write	member *	g:EnterpriseProjectId
elb:members:delete	Grants permission to remove a backend server.	write	member *	g:EnterpriseProjectId
elb:security-policies:list	Grants permission to query security policies.	list	securityPolicy *	-
			-	g:EnterpriseProjectId
elb:security-policies:show	Grants permission to query the details of a security policy.	read	securityPolicy *	-
elb:security-policies:create	Grants permission to create a security policy.	write	securityPolicy *	-
			-	g:EnterpriseProjectId
elb:security-policies:update	Grants permission to modify a security policy.	write	securityPolicy *	-
elb:security-policies:delete	Grants permission to delete a security policy.	write	securityPolicy *	-

Each ELB API usually supports one or more actions. **Table 5-50** lists the supported actions and dependencies.

Table 5-50 Actions and dependencies supported by ELB APIs

API	Action	Dependencies
GET /v3/{project_id}/elb/flavors	elb:flavors:list	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
POST /v3/{project_id}/elb/loadbalancers/{loadbalancer_id}/availability-zone/batch-add	elb:loadbalancers:update	-
POST /v3/{project_id}/elb/ipgroups	elb:ipgroups:create	-
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	-
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	-

API	Action	Dependencies
GET /v3/{project_id}/elb/security-policies	elb:security-policies:list	-
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	-

API	Action	Dependencies
GET /v3/{project_id}/elb/members	elb:members:list	-
POST /v3/{project_id}/elb/pools/{pool_id}/members/batch-add	elb:members:create	-
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	-

API	Action	Dependencies
POST /v3/{project_id}/elb/listeners	elb:listeners:create	-
DELETE /v3/{project_id}/elb/listeners/{listener_id}	elb:listeners:delete	-
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	-

API	Action	Dependencies
GET /v3/{project_id}/elb/preoccupy-ip-num	elb:loadbalancers:show	-
POST /v3/{project_id}/elb/logtanks	elb:logtanks:create	-
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/l7policies	elb:l7policies:create	-

API	Action	Dependencies
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	-
PUT /v3/{project_id}/elb/l7policies/{l7policy_id}/rules/{l7rule_id}	elb:l7rules:update	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-51**, 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 ELB.

Table 5-51 Resource types supported by ELB

Resource Type	URN
pool	elb:<region>:<account-id>:pool:<pool-id>
agreement	elb:<region>:<account-id>:agreement:<agreement-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>
subnet	vpc:<region>:<account-id>:subnet:<subnet-id>
listener	elb:<region>:<account-id>:listener:<listener-id>

Conditions

A Condition element lets you specify conditions for when an SCP 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, elb:) apply only to operations of ELB. For details, see **Table 5-52**.
  - 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 details about the supported operators, see operators.

The following table lists the condition keys that you can define in SCPs for ELB. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-52 Service-specific condition keys supported by ELB

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
elb:AssociatePublicips	boolean	Single valued	Filters access by whether an EIP is bound during load balancer creation or modification. If you want to control the public network access of a load balancer, you need to use the actions supported by EIP.

5.10.3.5 VPC Endpoint (VPCEP)

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 VPC Endpoint, 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 VPC Endpoint, see **Conditions**.

The following table lists the actions that you can define in SCP statements for VPC Endpoint.

Table 5-53 Actions Supported by VPC Endpoint

Action	Description	Access Level	Resource Type (*: required)	Condition Key
vpcep:endpoints:create	Grants permission to create a VPC endpoint for a specified service.	write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgPath • vpcep:VpceServiceOwner
			vpc *	-
			routeTable	-
			subnet	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
vpcep:endpoints:delete	Grants permission to delete a VPC endpoint.	write	endpoints *	• g:ResourceTag/<tag-key> • vpcep:VpceServiceName
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>
vpcep:endpoints:update	Grants permission to update the whitelist of a VPC endpoint.	write	endpoints *	• vpcep:VpceServiceName • vpcep:VpceServiceOrgPath • vpcep:VpceServiceOwner • g:ResourceTag/<tag-key>
			routeTable	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			subnet	-
vpcep:endpoints:updateRouteTables	Grants permission to modify route tables of a VPC endpoint.	write	endpoints *	g:ResourceTag/<tag-key>
			routeTable *	-
vpcep:endpoints:updatePolicy	Grants permission to modify a VPC endpoint policy.	write	endpoints *	g:ResourceTag/<tag-key>
vpcep:endpoints:deletePolicy	Grants permission to delete a VPC endpoint policy.	write	endpoints *	g:ResourceTag/<tag-key>
vpcep:endpointServices:create	Grants permission to create a VPC endpoint service.	write	endpointServices *	vpcep:VpceServicePrivateDnsName
			vpc *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
vpcep:endpointServices:list	Grants permission to query VPC endpoint services.	list	endpointServices *	-
			-	g:EnterpriseProjectId
vpcep:endpointServices:get	Grants permission to query details of a VPC endpoint service.	read	endpointServices *	g:ResourceTag/<tag-key>
vpcep:endpointServices:update	Grants permission to modify a VPC endpoint service.	write	endpointServices *	g:ResourceTag/<tag-key>
vpcep:endpointServices:delete	Grants permission to delete a VPC endpoint service.	write	endpointServices *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
vpcep:endpointServices:updateName	Grants permission to change the name of a VPC endpoint service.	write	endpointServices *	-
vpcep:endpointServices:describe	Grants permission to query basic information about a VPC endpoint service.	read	-	-
vpcep:endpointServices:listPublic	Grants permission to query public VPC endpoint services.	list	endpointServices *	-
vpcep:endpointServices:listPermissions	Grants permission to query whitelist records of a VPC endpoint service.	list	endpointServices *	-
vpcep:endpointServices:updatePermissions	Grants permission to batch add or delete whitelist records of a VPC endpoint service.	permission_management	endpointServices *	-
			-	• vpcep:VpceEndpointOrgPath • vpcep:VpceEndpointOwner
vpcep:endpointServices:createPermissions	Grants permission to batch add whitelist records of a VPC endpoint service.	permission_management	endpointServices *	-
			-	• vpcep:VpceEndpointOrgPath • vpcep:VpceEndpointOwner
vpcep:endpointServices:deletePermissions	Grants permission to batch delete whitelist records of a VPC endpoint service.	permission_management	endpointServices *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
vpcep:endpointServices:updatePermissionsDescription	Grants permission to update the whitelist description of a VPC endpoint service.	write	endpointServices *	-
vpcep:endpointServices:listConnections	Grants permission to query connections of a VPC endpoint service.	list	endpointServices *	-
vpcep:endpointServices:updateConnections	Grants permission to accept or reject a VPC endpoint.	write	endpointServices *	-
vpcep:endpointServices:updateConnectionDescription	Grants permission to update the description of a VPC endpoint connection.	write	endpointServices *	-
vpcep::listResourceTags	Grants permission to query resources by tag.	list	endpoints	-
			endpointServices	-
vpcep::updateResourceTags	Grants permission to batch add tags to or delete tags from a VPC endpoint service or VPC endpoint.	tagging	endpoints	-
			endpointServices	-
vpcep::getProjectTags	Grants permission to query resource tags of a tenant.	read	endpoints	-
			endpointServices	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
vpcep::listQuotas	Grants permission to query the quotas of your resources, including the quota of VPC endpoint services and the quota of VPC endpoints.	read	-	-
vpcep::listVersionDetails	Grants permission to query versions of VPC Endpoint APIs.	list	-	-
vpcep::listSpecifiedVersion	Grants permission to query information about a VPC Endpoint API version.	list	-	-

Each API of VPC Endpoint usually supports one or more actions. **Table 5-54** lists the supported actions and dependencies.

Table 5-54 Actions and dependencies supported by VPC Endpoint 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	-

API	Action	Dependencies
PUT /v1/{project_id}/vpc-endpoints/{vpc_endpoint_id}	vpcep:endpoints:update	-
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	-

API	Action	Dependencies
PUT /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/name	vpcep:endpointServices:updateName	-
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	-

API	Action	Dependencies
GET /v1/{project_id}/vpc-endpoint-services/{vpc_endpoint_service_id}/connections	vpcep:endpointServices:listConnections	-
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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-55**, a 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 VPC Endpoint.

Table 5-55 Resource types supported by VPC Endpoint

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

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, 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, **vpcep:**) apply only to operations of VPC Endpoint. For details, see **Table 5-56**.
  - 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 SCP 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 VPC Endpoint. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-56 Service-specific condition keys supported by VPC Endpoint

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
vpcep:VpceServiceName	string	Single-valued	Filters access by VPC endpoint service name.
vpcep:VpceServiceOwner	string	Single-valued	Filters access by VPC endpoint service owner.
vpcep:VpceServicePrivateDnsName	string	Single-valued	Filters access by the value of **VpceServicePrivateDnsName** that is passed in the request.
vpcep:VpceServiceOrgPath	string	Single-valued	Filters access by the organization path of the VPC endpoint service owner.
vpcep:VpceEndpointOrgPath	string	Single-valued	Filters access by the organization path of the VPC endpoint owner.
vpcep:VpceEndpointOwner	string	Single-valued	Filters access by the value of **accountId** of the VPC endpoint owner.
vpcep:VpcId	string	Multivalued	Filters accesses by VPC ID.

5.10.3.6 Direct Connect (DC)

The Organizations service provides Service Control Policies 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 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 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 Direct Connect, 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 Direct Connect, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Direct Connect.

Table 5-57 Actions supported by Direct Connect

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dcaas:directConnect:create	Grants permission to create a connection.	write	directConnect *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dcaas:directConnect:update	Grants permission to update a connection.	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:delete	Grants permission to delete a connection. This action can only be used by pay-per-use connections. You can only unsubscribe from yearly/monthly connections.	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:get	Grants permission to query details of a connection.	read	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:list	Grants permission to list the connections.	list	directConnect *	-
			-	g:EnterpriseProjectId
dcaas:directConnect:createHostedDirectConnect	Grants permission to allow a partner to create a hosted connection.	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:updateHostedDirectConnect	Grants permission to allow a partner to update a hosted connection.	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:deleteHostedDirectConnect	Grants permission to allow a partner to delete a hosted connection.	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dcaas:directConnect:getHostedDirectConnect	Grants permission to allow a partner to query details of a hosted connection.	read	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:listHostedDirectConnect	Grants permission to allow a partner to list the hosted connections.	list	directConnect *	g:EnterpriseProjectId
dcaas:directConnect:createOnestopDirectConnect	Grants permission to create a full-service connection.	write	directConnect *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dcaas:directConnect:updateOnestopDirectConnect	Grants permission to update a full-service connection.	write	directConnect *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:directConnect:createOrder	Grants permission to create an order for a connection.	write	directConnect *	-
dcaas:directConnect:updateOrder	Grants permission to modify the order for changing the specifications of a connection.	write	directConnect *	-
dcaas:vgw:create	Grants permission to create a virtual gateway.	write	vgw *	-
			vpc	-
			instances	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
dcaas:vgw:update	Grants permission to update a virtual gateway.	write	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vgw:delete	Grants permission to delete a virtual gateway.	write	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vgw:get	Grants permission to query details of a virtual gateway.	read	vgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vgw:list	Grants permission to list the virtual gateways.	list	vgw *	-
			-	g:EnterpriseProjectId
dcaas:vif:create	Grants permission to create a virtual interface.	write	vif *	-
			directConnect	-
			lag	-
			vgw	-
			gdgw	-
			connectGateway	-
			lgw	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dcaas:vif:update	Grants permission to update a virtual interface.	write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vif:delete	Grants permission to delete a virtual interface.	write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vif:get	Grants permission to query details of a virtual interface.	read	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:vif:list	Grants permission to list the virtual interfaces.	list	vif *	-
			-	g:EnterpriseProjectId
dcaas:vif:updateVifExtendAttribute	Grants permission to update extended attributes of a virtual interface.	write	vif *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dcaas:gdgw:create	Grants permission to create a global DC gateway.	write	gdgw *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
dcaas:gdgw:update	Grants permission to update a global DC gateway.	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:delete	Grants permission to delete a global DC gateway.	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:get	Grants permission to query details of a global DC gateway.	read	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:list	Grants permission to list the global DC gateways.	list	gdgw *	-
			-	g:EnterpriseProjectId
dcaas:gdgw:createPeerlink	Grants permission to create a peer link for a global DC gateway.	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:updatePeerlink	Grants permission to update a peer link of a global DC gateway.	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:deletePeerlink	Grants permission to delete a peer link of a global DC gateway.	write	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dcaas:gdgw:getPeerlink	Grants permission to query details of a peer link of a global DC gateway.	read	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
dcaas:gdgw:listPeerlink	Grants permission to list the peer links of a global DC gateway.	list	gdgw *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
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	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcaas:resources:listResourceTag	Grants permission to query tags of a resource.	list	directConnect	-
			lag	-
			vgw	-
			vif	-
			gdgw	-
dcaas:resources:listTag	Grants permission to query tags by resource type.	list	directConnect	-
			lag	-
			vgw	-
			vif	-
			gdgw	-
dcaas:resources:tag	Grants permission to add a tag to a resource.	tagging	directConnect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcaas:resources:unTag	Grants permission to delete a tag from a resource.	tagging	directConnect	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			lag	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			vif	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			gdgw	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
dcaas:resources:listByTag	Grants permission to query resources by tag.	list	directConnect	-
			lag	-
			vgw	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			vif	-
			gdgw	-
dcaas:gdgw:listGdgwRouteTable	Grants permission to query a custom route table of a global DC gateway.	list	gdgw *	-
dcaas:gdgw:updateGdgwRouteTable	Grants permission to update a custom route table of a global DC gateway.	write	gdgw *	-
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	-	-

Each API of Direct Connect usually supports one or more actions. **Table 5-58** lists the supported actions and dependencies.

Table 5-58 Actions and dependencies supported by Direct Connect 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	-

API	Action	Dependencies
DELETE /v3/{project_id}/dcaas/direct-connects/{direct_connect_id}	dcaas:directConnect:delete	-
GET /v3/{project_id}/dcaas/hosted-connects/{hosted_connect_id}	dcaas:directConnect:getHostedDirectConnect	-
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	er:instances:get vpc:vpcs:get

API	Action	Dependencies
GET /v3/{project_id}/dcaas/virtual-interfaces/{virtual_interface_id}	dcaas:vif:get	-
GET /v3/{project_id}/dcaas/virtual-interfaces	dcaas:vif:list	-
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	-
POST /v3/{project_id}/dcaas/switchover-test	dcaas:vif:switchoverTest	-
GET /v3/{project_id}/dcaas/switchover-test	dcaas:vif:listSwitchoverTestRecord	-
GET /v3/{project_id}/dcaas/quotas	dcaas:quota:listUsage	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-59**, 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 Direct Connect.

Table 5-59 Resource types supported by Direct Connect

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

Direct Connect does not support service-specific condition keys in SCPs. Direct Connect can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.3.7 Enterprise Router (ER)

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 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 Enterprise Router, 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 Enterprise Router, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Enterprise Router.

Table 5-60 Actions supported by Enterprise Router

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
er:instances:get	Grants permission to query the details of an enterprise router.	read	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:create	Grants permission to create an enterprise router.	write	instances *	g:EnterpriseProjectId	-
			-	• g:RequestTag/<tag-key> • g:TagKeys	
er:instances:list	Grants permission to list the enterprise routers.	list	instances *	-	-
er:instances:update	Grants permission to update an enterprise router.	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:delete	Grants permission to delete an enterprise router.	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:instances:createVpcAttachment	Grants permission to create a VPC attachment.	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:create
er:instances:showVpcAttachment	Grants permission to query the details of a VPC attachment.	read	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:get

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
er:instances:listVpcAttachments	Grants permission to list the VPC attachments.	list	instances *	-	er:attachments:list
er:instances:updateVpcAttachment	Grants permission to update a VPC attachment.	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:update
er:instances:deleteVpcAttachment	Grants permission to delete a VPC attachment.	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:delete
er:commonAttachments:get	Grants permission to query the details of an attachment.	read	attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:get
er:commonAttachments:list	Grants permission to query the attachment list.	list	attachments *	-	er:attachments:list
er:commonAttachments:update	Grants permission to update an attachment.	write	attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:attachments:update
er:routeTables:get	Grants permission to query the details of a route table.	read	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:create	Grants permission to create a route table.	write	routeTables *	-	-
			instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			-	• g:RequestTag/<tag-key> • g:TagKeys	
er:routeTables:list	Grants permission to list the route tables.	list	routeTables *	-	-
er:routeTables:update	Grants permission to update a route table.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:delete	Grants permission to delete a route table.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
er:routeTables:associate	Grants permission to associate an attachment with a route table.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:associate
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:disassociate	Grants permission to disassociate an attachment from a route table.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:disassociate
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:listAssociations	Grants permission to list the associations.	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:associations:list

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
er:routeTables:enablePropagation	Grants permission to allow an attachment to propagate routes to the specified propagation route table.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:enable
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:disablePropagation	Grants permission to prohibit an attachment from propagating routes to the specified propagation route table.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:disable
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:routeTables:listPropagations	Grants permission to list the propagations.	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:propagations:list
er:staticRoutes:list	Grants permission to list the static routes.	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:list
er:staticRoutes:create	Grants permission to create a static route.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:create
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:effectiveRoutes:list	Grants permission to list the effective routes.	list	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:list

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
er:staticRoutes:delete	Grants permission to delete a static route.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:delete
er:staticRoutes:update	Grants permission to update a static route.	write	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:update
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:staticRoutes:get	Grants permission to query a static route.	read	routeTables *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:routes:get
er:tags:singleCreate	Grants permission to create a resource tag.	write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:tags:create
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:delete	Grants permission to delete a resource tag.	write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:batchOperation	Grants permission to add tags in batches.	write	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	er:tags:create
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:get	Grants permission to query tags of a specific resource.	read	routeTables	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			instances	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			attachments	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
er:tags:list	Grants permission to list the tags.	list	-	-	-
er:quotas:list	Grants permission to query resource quotas.	list	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
er:flowLogs:create	Grants permission to create a flow log.	write	instances *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	-
			attachments *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	
			flowLogs *	-	
er:flowLogs:list	Grants permission to list the flow logs.	list	flowLogs *	-	-
er:flowLogs:get	Grants permission to query the details of a flow log.	read	flowLogs *	-	-
er:flowLogs:update	Grants permission to update a flow log.	write	flowLogs *	-	-
er:flowLogs:delete	Grants permission to delete a flow log.	write	flowLogs *	-	-
er:flowLogs:enable	Grants permission to enable flow logging.	write	flowLogs *	-	-
er:flowLogs:disable	Grants permission to disable flow logging.	write	flowLogs *	-	-

Each API of Enterprise Router usually supports one or more actions. **Table 5-61** lists the supported actions and dependencies.

Table 5-61 Actions and dependencies supported by Enterprise Router APIs

API	Action	Dependency
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	-
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	-
GET /v3/{project_id}/enterprise-router/{er_id}/vpc-attachments/{vpc_attachment_id}	er:instances:showVpcAttachment	-
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:deleteVpcAttachment	-
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}/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	-

API	Action	Dependency
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	-
GET /v3/{project_id}/enterprise-router/{er_id}/route-tables/{route_table_id}/propagations	er:routeTables:listPropagations	-
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	-

API	Action	Dependency
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	-
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 SCP policy applies to. If you specify a resource type for any action in **Table 5-62**, 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 policy to define resource types.

The following table lists the resource types that you can define in SCP statements for Enterprise Router.

Table 5-62 Resource types supported by Enterprise Router

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>:flowFlogs:<flow-log-id>
attachments	er:<region>:<account-id>:attachments:<attachment-id>

Conditions

Enterprise Router does not support service-specific condition keys in an SCP.

Enterprise Router can only use global condition keys applicable to all services. For details, see Global Condition Keys

5.10.3.8 Global Accelerator (GA)

The Organizations service provides Service Control Policies 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 topic 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 (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 SCP 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 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 Global Accelerator, 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 Global Accelerator, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Global Accelerator.

Table 5-63 Actions supported by Global Accelerator

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
ga:accelerator:list	Grants permission to query global accelerators.	list	accelerator *	-
ga:accelerator:create	Grants permission to create a global accelerator.	write	accelerator *	g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
ga:accelerator:get	Grants permission to query the details of a global accelerator.	read	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
ga:accelerator:update	Grants permission to update a global accelerator.	write	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ga:accelerator:delete	Grants permission to delete a global accelerator.	write	accelerator *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ga:listener:list	Grants permission to query listeners.	list	listener *	-
ga:listener:create	Grants permission to add a listener.	write	listener *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
ga:listener:get	Grants permission to query the details of a listener.	read	listener *	g:ResourceTag/<tag-key>
ga:listener:update	Grants permission to modify a listener.	write	listener *	g:ResourceTag/<tag-key>
ga:listener:delete	Grants permission to delete a listener.	write	listener *	g:ResourceTag/<tag-key>
ga:endpointgroup:list	Grants permission to query endpoint groups.	list	endpointgroup *	-
ga:endpointgroup:create	Grants permission to add an endpoint group.	write	endpointgroup *	-
			-	ga:RequestRegionId
ga:endpointgroup:get	Grants permission to query the details of an endpoint group.	read	endpointgroup *	ga:RegionId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 query endpoints.	list	endpoint *	-
ga:endpoint:create	Grants permission to add an endpoint.	write	endpoint *	-
			-	• ga:RequestResourceType • ga:RequestResourceId • ga:RequestIpAddress • ga:RequestDomainName
ga:endpoint:get	Grants permission to query the details of an endpoint.	read	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName
ga:endpoint:update	Grants permission to modify an endpoint.	write	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName
ga:endpoint:delete	Grants permission to remove an endpoint.	write	endpoint *	• ga:ResourceType • ga:ResourceId • ga:IpAddress • ga:DomainName

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
ga:healthcheck:list	Grants permission to query health checks.	list	healthcheck *	-
ga:healthcheck:create	Grants permission to configure a health check.	write	healthcheck *	-
ga:healthcheck:get	Grants permission to query health check details.	read	healthcheck *	-
ga:healthcheck:update	Grants permission to modify a health check.	write	healthcheck *	-
ga:healthcheck:delete	Grants permission to delete a health check.	write	healthcheck *	-
ga:tag:create	Grants permission to add tags in batches.	tagging	accelerator	g:ResourceTag/<tag-key>
			listener	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
ga:tag:delete	Grants permission to delete tags in batches.	tagging	accelerator *	g:ResourceTag/<tag-key>
			listener *	g:ResourceTag/<tag-key>
			-	g:TagKeys
ga:tag:get	Grants permission to query tags of a specific resource.	read	accelerator	g:ResourceTag/<tag-key>
			listener	g:ResourceTag/<tag-key>
ga:tag:list	Grants permission to query the tags.	list	-	-
ga::listResourcesByTag	Grants permission to query resources by tag.	list	-	g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
ga:ipgroup:list	Grants permission to query IP address groups.	list	ipgroup *	-
ga:ipgroup:create	Grants permission to create an IP address group.	write	ipgroup *	-
ga:ipgroup:get	Grants permission to query the details of an IP address group.	read	ipgroup *	-
ga:ipgroup:update	Grants permission to modify an IP address group.	write	ipgroup *	-
ga:ipgroup:delete	Grants permission to delete an IP address group.	write	ipgroup *	-
ga:ipgroup:addIps	Grants permission to add IP addresses to an IP address group in batches.	write	ipgroup *	-
ga:ipgroup:removeIps	Grants permission to remove IP addresses from an IP address group in batches.	write	ipgroup *	-
ga:ipgroup:associateListener	Grants permission to associate an IP address group with a listener.	write	ipgroup *	-
ga:ipgroup:disassociateListener	Grant permission to disassociate an IP address group from a listener.	write	ipgroup *	-
ga::listByoipPools	Grants permission to query your own IP address pools.	list	-	-
ga:logtank:list	Grants permission to query logs.	list	logtank *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
ga:logtank:create	Grants permission to create a log.	write	logtank *	-
ga:logtank:get	Grants permission to query the details of a log.	read	logtank *	-
ga:logtank:update	Grants permission to modify a log.	write	logtank *	-
ga:logtank:delete	Grants permission to delete a log.	write	logtank *	-

Each API of Global Accelerator usually supports one or more actions. **Table 5-64** lists the supported actions and dependencies.

Table 5-64 Actions and dependencies supported by Global Accelerator APIs

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

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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 SCP is applied. If you specify a resource type for any action in **Table 5-65**, the resource URN must be specified in the SCP statements using that action, and the SCP only applies 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 policy to define resource types.

The following table lists the resource types that you can define in SCP statements for Global Accelerator.

Table 5-65 Resource types supported by Global Accelerator

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

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, ga:) only apply to operations of Global Accelerator. For details, see **Table 5-66**.
  - 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.

The following table lists the condition keys that you can define in SCPs for Global Accelerator. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-66 Service-specific condition keys supported by Global Accelerator

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
ga:RequestRegionId	string	Single-valued	Filters access by region ID passed in the request.
ga:RequestResource-Type	string	Single-valued	Filters access by resource type passed in the request.
ga:RequestResourceId	string	Single-valued	Filters access by resource ID passed in the request.
ga:RequestIpAddress	string	Single-valued	Filters access by IP address passed in the request.
ga:RequestDomainName	string	Single-valued	Filters access by domain name passed in the request.
ga:RegionId	string	Single-valued	Filters access by region of the endpoint group.
ga:ResourceType	string	Single-valued	Filters access by resource type of the endpoint group.
ga:ResourceId	string	Single-valued	Filters access by resource ID of the endpoint group.
ga:IpAddress	string	Single-valued	Filters access by IP address of the endpoint group.
ga:DomainName	string	Single-valued	Filters access by domain name of the endpoint group.

5.10.3.9 Cloud Connect (CC)

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 (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 SCP 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 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 Cloud Connect, 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 Cloud Connect, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Cloud Connect.

Table 5-67 Actions supported by Cloud Connect

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:cloudConnections:create	Grants permission to create a cloud connection.	write	cloudConnection *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
cc:cloudConnections:delete	Grants permission to delete a cloud connection.	write	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:cloudConnections:update	Grants permission to update a cloud connection.	write	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:cloudConnections:get	Grants permission to query the details of a cloud connection.	read	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:cloudConnections:list	Grants permission to list the cloud connections.	list	cloudConnection *	-
cc:cloudConnections:tag	Grants permission to add tags to a cloud connection.	tagging	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:cloudConnections:unTag	Grants permission to delete tags from a cloud connection.	tagging	cloudConnection *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:cloudConnections:listTags	Grants permission to list the tags added to a cloud connection.	list	cloudConnection *	-
cc:networkInstances:create	Grants permission to load a network instance.	write	networkInstance *	-
			cloudConnection *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId
cc:networkInstances:delete	Grants permission to remove a network instance.	write	networkInstance *	• cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:networkInstances:update	Grants permission to update a network instance.	write	networkInstance *	• cc:VpcId • cc:VirtualGatewayId • cc:EnterpriseRouterId
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:networkInstances:get	Grants permission to query the details of a network instance.	read	networkInstance *	-
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:networkInstances:list	Grants permission to list the network instances.	list	networkInstance *	-
cc:bandwidthPackages:create	Grants permission to create a bandwidth package.	write	bandwidthPackage *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
cc:bandwidthPackages:delete	Grants permission to delete a bandwidth package.	write	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:bandwidthPackages:update	Grants permission to update a bandwidth package.	write	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:bandwidthPackages:get	Grants permission to query the details of a bandwidth package.	read	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:bandwidthPackages:list	Grants permission to list the bandwidth packages.	list	bandwidthPackage *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:bandwidthPackages:tag	Grants permission to add tags to a bandwidth package.	tagging	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:bandwidthPackages:unTag	Grants permission to delete tags from a bandwidth package.	tagging	bandwidthPackage *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:bandwidthPackages:listTags	Grants permission to list the tags added to a bandwidth package.	list	bandwidthPackage *	-
cc:bandwidthPackages:associate	Grants permission to bind a bandwidth package to a cloud connection.	write	bandwidthPackage *	g:ResourceTag/<tag-key>
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:bandwidthPackages:disassociate	Grants permission to unbind a bandwidth package from a cloud connection.	write	bandwidthPackage *	g:ResourceTag/<tag-key>
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:interRegionBandwidths:create	Grants permission to assign an inter-region bandwidth.	write	interRegionBandwidth *	-
			cloudConnection *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • cc:BandwidthPackageId
cc:interRegionBandwidths:delete	Grants permission to delete an inter-region bandwidth.	write	interRegionBandwidth *	cc:BandwidthPackageId
			cloudConnection *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
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

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:interRegionBandwidths:list	Grants permission to list 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 list the cloud connection routes.	list	-	-
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 list 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
cc:authorisation:listPermissions	Grants permission to list the VPCs that other accounts allow you to load to your cloud connection.	list	-	-
cc:centralNetwork:create	Grants permission to create a central network.	write	central Network *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • cc:MultipleEnterpriseRouterIds
cc:centralNetwork:delete	Grants permission to delete a central network.	write	central Network *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:update	Grants permission to update a central network.	write	central Network *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:centralNetwork:get	Grants permission to query the details of a central network.	read	central Network *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:list	Grants permission to list the central networks.	list	central Network *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:centralNetwork:tag	Grants permission to add tags to a central network.	tagging	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:centralNetwork:unTag	Grants permission to delete tags from a central network.	tagging	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cc:centralNetwork:listTags	Grants permission to list the tags added to a central network.	list	centralNetwork *	-
cc:centralNetwork:createPolicy	Grants permission to add a policy to a central network.	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	cc:MultipleEnterpriseRouterIds
cc:centralNetwork:applyPolicy	Grants permission to apply a policy to a central network.	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:deletePolicy	Grants permission to delete a policy from a central network.	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cc:centralNetwork:listPolicies	Grants permission to list the central network policies.	list	centralNetwork *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:centralNetwork:listChangeSet	Grants permission to query the changes between the current policy and the applied policy.	list	centralNetwork *	-
cc:centralNetwork:listConnections	Grants permission to list the central network connections.	list	centralNetwork *	-
cc:centralNetwork:updateConnection	Grants permission to update a central network connection.	write	centralNetwork *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	cc:GlobalConnectionBandwidthId
cc:centralNetworkAttachment:createGdgw	Grants permission to add a global DC gateway to a central network as an attachment.	write	centralNetworkAttachment *	-
			centralNetwork *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • cc:EnterpriseRouterId • cc:GlobalDcGatewayId
cc:centralNetworkAttachment:updateGdgw	Grants permission to update a global DC gateway on a central network.	write	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:centralNetworkAttachment:getGdgw	Grants permission to query the details of a global DC gateway on a central network.	read	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:listGdgws	Grants permission to list 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>
			-	• g:EnterpriseProjectId • cc:MultipleEnterpriseRouterIds
cc:centralNetworkAttachment:updateErRouteTable	Grants permission to update an enterprise router route table on a central network.	write	centralNetworkAttachment *	cc:MultipleEnterpriseRouterIds
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cc:centralNetworkAttachment:getErRouteTable	Grants permission to query the details of an enterprise router route table on a central network.	read	centralNetworkAttachment *	cc:MultipleEnterpriseRouterIds
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:listErRouteTables	Grants permission to list the enterprise router route tables on a central network.	list	centralNetworkAttachment *	-
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:delete	Grants permission to delete an attachment from a central network.	write	centralNetworkAttachment *	• cc:GlobalDcGatewayId • cc:EnterpriseRouterId • cc:MultipleEnterpriseRouterIds
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
cc:centralNetworkAttachment:list	Grants permission to list the central network attachments.	list	centralNetworkAttachment *	-
			centralNetwork *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Each API of Cloud Connect usually supports one or more actions. **Table 5-68** lists the supported actions and dependencies.

Table 5-68 Actions and dependencies supported by Cloud Connect 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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
GET /v3/{domain_id}/ccaas/cloud-connection-routes	cc:cloudConnection-Routes:list	-
POST /v3/{domain_id}/ccaas/authorisations	cc:authorisation:create	-
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	-

API	Action	Dependencies
POST /v3/{domain_id}/gcn/central-networks	cc:centralNetwork:create	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
DELETE /v3/{domain_id}/gcn/central-networks/{central_network_id}	cc:centralNetwork:delete	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
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	-

API	Action	Dependencies
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	-
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	• er:instances:get • er:routeTables:get
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/policies/{policy_id}/apply	cc:centralNetwork:applyPolicy	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
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	-

API	Action	Dependencies
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	-
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	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
PUT /v3/{domain_id}/gcn/central-network/{central_network_id}/gdgw-attachments/{gdgw_attachment_id}	cc:centralNetworkAttachment:updateGdgw	-

API	Action	Dependencies
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	-
POST /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments	cc:centralNetworkAttachment:createErRouteTable	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
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	-

API	Action	Dependencies
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/er-route-table-attachments	cc:centralNetworkAttachment:listErRouteTables	-
DELETE /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments/{attachment_id}	cc:centralNetworkAttachment:delete	• er:instances:get • er:routeTables:get • er:routeTables:listPropagations • er:routeTables:enablePropagation • er:routeTables:disablePropagation • er:routeTables:listAssociations • er:routeTables:associate • er:routeTables:disassociate
GET /v3/{domain_id}/gcn/central-network/{central_network_id}/attachments	cc:centralNetworkAttachment:list	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-69**, 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 policy to define resource types.

The following table lists the resource types that you can define in SCP statements for Cloud Connect.

Table 5-69 Resource types supported by Cloud Connect

Resource Type	URN
cloudConnection	cc::<account-id>:cloudConnection:<cloud-connection-id>
interRegionBandwidth	cc::<account-id>:interRegionBandwidth:<inter-region-bandwidth-id>

Resource Type	URN
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

A Condition element lets you specify conditions for when an SCP 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, cc:) apply only to operations of Cloud Connect. For details, see **Table 5-70**.
  - 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 details about the supported operators, see operators.

The following table lists the condition keys that you can define in SCPs for Cloud Connect. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-70 Service-specific condition keys supported by Cloud Connect

Service-specific Condition Key	Type	Single-valued/ Multivalued	What To Do
cc:VpcId	string	Single-valued	VPC ID as a filter.
cc:VirtualGatewayId	string	Single-valued	Direct Connect virtual gateway ID as a filter.
cc:EnterpriseRouterId	string	Single-valued	Enterprise router ID as a filter.
cc:MultipleEnterpriseRouterIds	string	Multivalued	Enterprise router IDs as a filter.
cc:BandwidthPackageId	string	Single-valued	Bandwidth package ID as a filter.
cc:GlobalConnectionBandwidthId	string	Single-valued	Global private bandwidth ID as a filter.
cc:GlobalDcGatewayId	string	Single-valued	Global DC gateway ID as a filter.

5.10.4 Containers

5.10.4.1 Cloud Container Engine (CCE)

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 CCE, 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 CCE, see **Conditions**.

The following table lists the actions that you can define in SCP statements for CCE.

Table 5-71 Actions Supported by CCE

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cce:cluster:createCluster	Grants permission to create a cluster.	write	cluster *	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>
cce:cluster:delete	Grants permission to delete a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:updateCluster	Grants permission to update a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:upgrade	Grants permission to upgrade the version of a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cce:cluster:start	Grants permission to wake up a hibernated cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:stop	Grants permission to hibernate a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:list	Grants permission to view the cluster details list.	list	cluster *	-
cce:cluster:getCluster	Grants permission to view details about a specified cluster.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cce:cluster:getEndpoints	Grants permission to view the access address of a specified cluster.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cce:cluster:resize	Grants permission to modify the specifications of a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:eipBinding	Grants permission to bind or unbind a public IP address to or from a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:generateClientCredential	Grants permission to generate cluster client access credentials.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:addTags	Grants permission to add tags to a cluster.	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:TagKeys • g:RequestTag/<tag-key>
cce:cluster:removeTags	Grants permission to delete tags from a cluster.	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
cce:cluster:getConfigurationTemplate	Grants permission to obtain the configuration template information about a cluster.	read	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:cluster:getLogConfig	Grants permission to obtain the current log collection configurations of a cluster.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:cluster:updateLogConfig	Grants permission to update the log collection configurations of a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cce:partition:create	Grants permission to access a partition.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:partition:update	Grants permission to update a partition.	write	cluster *	g:EnterpriseProjectId
cce:partition:get	Grants permission to obtain details about a specified partition.	read	cluster *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cce:partition:list	Grants permission to view the partition list in a specified cluster.	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:nodepool:create	Grants permission to create a node pool.	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:nodepool:delete	Grants permission to delete a node pool.	write	cluster *	g:EnterpriseProjectId
cce:nodepool:updateNodepool	Grants permission to update a node pool.	write	cluster *	-
			-	• evs:Encrypted • g:EnterpriseProjectId
cce:nodepool:getNodepool	Grants permission to obtain details about a specified node pool.	read	cluster *	g:EnterpriseProjectId
cce:nodepool:list	Grants permission to view the node pool list in a specified cluster.	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:nodepool:getConfigurationTemplate	Grants permission to obtain node pool configuration templates.	read	cluster *	g:EnterpriseProjectId
cce:nodepool:getConfiguration	Grants permission to obtain the configurations of a node pool.	read	cluster *	g:EnterpriseProjectId
cce:nodepool:updateConfiguration	Grants permission to update the configurations of a node pool.	write	cluster *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cce:node:createNode	Grants permission to create a node.	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:node:delete	Grants permission to delete a node.	write	cluster *	g:EnterpriseProjectId
cce:node:update	Grants permission to update a node.	write	cluster *	g:EnterpriseProjectId
cce:node:getNode	Grants permission to obtain details about a specified node.	read	cluster *	g:EnterpriseProjectId
cce:node:list	Grants permission to view the node list in a specified cluster.	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:node:reset	Grants permission to reset a node.	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:node:add	Grants permission to manage a node.	write	cluster *	• cce:ClusterId • evs:Encrypted • g:EnterpriseProjectId
cce:node:remove	Grants permission to release a node.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:node:migrate	Grants permission to migrate nodes between clusters.	write	cluster *	• cce:nodeTransferSourceCluster • cce:nodeTransferTargetCluster • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cce:node:sync	Grants permission to synchronize infrastructure and resource status between nodes.	read	cluster *	g:EnterpriseProjectId
cce:quota:get	Grants permission to obtain resource quotas of cloud services used in a CCE cluster.	read	-	-
cce:addonInstance:create	Grants permission to create an add-on instance.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:delete	Grants permission to delete an add-on instance.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:update	Grants permission to update an add-on instance.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:get	Grants permission to obtain details about a specified add-on instance.	read	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:list	Grants permission to view the add-on instance list in a specified cluster.	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:addonInstance:rollback	Grants permission to roll back a specified add-on instance.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:chart:upload	Grants permission to upload an application chart.	write	-	-
cce:chart:delete	Grants permission to delete an application chart.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cce:chart:update	Grants permission to update an application chart.	write	-	-
cce:chart:listChart	Grants permission to view the application chart details list.	list	-	-
cce:chart:getChart	Grants permission to view details about an application chart specified by a user.	read	-	-
cce:chart:download	Grants permission to view the application charts downloaded by a user.	read	-	-
cce:chart:getQuota	Grants permission to view the application chart quota.	read	-	-
cce:release:create	Grants permission to create a release.	write	-	• cce:ClusterId • g:EnterpriseProjectId
cce:release:delete	Grants permission to delete a release.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:release:update	Grants permission to update a release.	write	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:release:get	Grants permission to obtain details about a specified release.	read	cluster *	• cce:ClusterId • g:EnterpriseProjectId
cce:release:list	Grants permission to view the release list in a specified cluster.	list	cluster *	• cce:ClusterId • g:EnterpriseProjectId

Each API of CCE usually supports one or more actions. **Table 5-72** lists the supported actions and dependencies.

Table 5-72 Actions and dependencies supported by CCE APIs

API	Action	Dependencies
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/upgradeworkflows	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id}	cce:cluster:upgrade	-

API	Action	Dependencies
PATCH /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgradeworkflows/{upgrade_workflow_id}	cce:cluster:upgrade	-
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:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/continue	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/pause	cce:cluster:upgrade	-
GET /api/v3/clusterupgradefeaturegates	cce:cluster:upgrade	-

API	Action	Dependencies
GET /api/v3/clusterupgradepaths	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/upgradeinfo	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/postcheck	cce:cluster:upgrade	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/precheck/tasks/{task_id}	cce:cluster:upgrade	-
GET /api/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot/tasks	cce:cluster:upgrade	-

API	Action	Dependencies
POST /api/v3.1/projects/{project_id}/clusters/{cluster_id}/operation/snapshot	cce:cluster:upgrade	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/upgrade/tasks	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	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/operation/resize	cce:cluster:resize	-

API	Action	Dependencies
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/mastereip	cce:cluster:eipBinding	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/clustercert	cce:cluster:generateClientCredential	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/tags/create	cce:cluster:addTags	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/tags/delete	cce:cluster:removeTags	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/configuration/detail	cce:cluster:getConfigurationTemplate	-
GET /api/v3/projects/{project_id}/cluster/{cluster_id}/log-configs	cce:cluster:getLogConfig	-
PUT /api/v3/projects/{project_id}/cluster/{cluster_id}/log-configs	cce:cluster:updateLogConfig	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/partitions	cce:partition:create	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration/detail	cce:nodepool:getConfigurationTemplate	-
GET /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration	cce:nodepool:getConfiguration	-
PUT /api/v3/projects/{project_id}/clusters/{cluster_id}/nodepools/{nodepool_id}/configuration	cce:nodepool:updateConfiguration	-
POST /api/v3/projects/{project_id}/clusters/{cluster_id}/nodes	cce:node:createNode	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-
GET /v2/charts/{project_id}/quotas	cce:chart:getQuota	-

API	Action	Dependencies
POST /cce/cam/v3/clusters/{cluster_id}/releases	cce:release:create	-
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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-73**, 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 CCE.

Table 5-73 Resource types supported by CCE

Resource Type	URN
cluster	cce:<region>:<account-id>:cluster:<cluster-name>

Conditions

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, cce:) only apply to operations of the CCE service. For details, see **Table 5-74**.
  - 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.

The following table lists the condition keys that you can define in SCPs for CCE. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-74 Service-specific condition keys supported by CCE

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
cce:ClusterId	string	Single-valued	Obtains access permissions based on the cluster ID transferred in a request.
cce:nodeTransferSourceCluster	string	Single-valued	Obtains access permissions based on the ID of the source cluster from which a node is migrated.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
cce:nodeTransferTargetCluster	string	Single-valued	Obtains access permissions based on the ID of the destination cluster to which a node is migrated.
cce:AssociatePublicIp	string	Single-valued	Obtains access permissions based on whether the ECS creation involves automatic EIP creation. To restrict the permission to bind or unbind EIPs to or from a cluster, use the cce:cluster:eipBinding action.
cce:VpcId	string	Single-valued	Obtains access permissions based on the VPC selected during cluster creation.
cce:SubnetId	string	Single-valued	Obtains access permissions based on the subnet selected during cluster, node, or node pool creation.
cce:Subnets	array	Single-valued	Obtains access permissions based on the subnets selected during node pool creation or updates.
cce:KmsKeys	string	Single-valued	Obtains access permissions based on the KMS key selected for disk encryption during node or node pool creation.

5.10.4.2 SoftWare Repository for Container (SWR)

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 SWR, 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 SWR, see **Conditions**.

The following table lists the actions that you can define in SCP statements for SWR.

Table 5-75 Actions supported by SWR

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:namespace:createNamespace	(Shared Edition) Grants permission to create an organization.	Write	namespace *	-
swr:namespace:deleteNamespace	(Shared Edition) Grants permission to delete an organization.	Write	namespace *	-
swr:namespace:listNamespaces	(Shared Edition) Grants permission to list organizations.	List	namespace *	-
swr:namespace:getNamespace	(Shared Edition) Grants permission to query details about an organization.	Read	namespace *	-
swr:repo:createRepo	(Shared Edition) Grants permission to create a repository.	Write	repo *	-
			-	swr:AllowPublicAccess
swr:repo:deleteRepo	(Shared Edition) Grants permission to delete a repository.	Write	repo *	-
swr:repo:listRepos	(Shared Edition) Grants permission to list repositories.	List	repo *	-
swr:repo:listSharedRepos	(Shared Edition) Grants permission to list shared images.	List	repo *	-
swr:repo:getRepo	(Shared Edition) Grants permission to query brief information about a repository.	Read	repo *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repo:updateRepo	(Shared Edition) Grants permission to update brief information about a repository.	Write	repo *	-
			-	swr:AllowPublicAccess
swr:repo:deleteRepoTag	(Shared Edition) Grants permission to delete images with specified tags.	Write	repo *	-
swr:repo:createRepoTag	(Shared Edition) Grants permission to create an image tag.	Write	repo *	-
swr:repo:listRepoTags	(Shared Edition) Grants permission to list image tags.	List	repo *	-
swr:repo:createRepoDomain	(Shared Edition) Grants permission to share images with other accounts.	Permission_management	repo *	-
			-	• swr:TargetAccountId • swr:TargetOrgPath • swr:TargetOrgId
swr:repo:deleteRepoDomain	(Shared Edition) Grants permission to delete accounts from an image sharing list.	Permission_management	repo *	-
swr:repo:listRepoDomains	(Shared Edition) Grants permission to list accounts an image is shared with.	List	repo *	-
swr:repo:getRepoDomain	(Shared Edition) Grants permission to check whether images are shared with an account.	Read	repo *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repo:updateRepoDomain	(Shared Edition) Grants permission to update an account images are shared with.	Permission_management	repo *	-
swr:repo:createRepoShare	(Shared Edition) Grants permission to create an image sharing policy.	Permission_management	repo *	-
			-	• swr:TargetAccountId • swr:TargetOrgPath • swr:TargetOrgId
swr:repo:deleteRepoShare	(Shared Edition) Grants permission to delete an image sharing policy.	Permission_management	repo *	-
swr:repo:listRepoShares	(Shared Edition) Grants permission to list image sharing policies.	List	repo *	-
swr:repo:getRepoShare	(Shared Edition) Grants permission to query details about an image sharing policy.	Read	repo *	-
swr:repo:updateRepoShare	(Shared Edition) Grants permission to update an image sharing policy.	Permission_management	repo *	-
swr:repo:createAutoSyncRepoJob	(Shared Edition) Grants permission to create an automatic image synchronization task.	Write	repo *	-
			-	swr:TargetRegion

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repo:createManualSyncRepoJob	(Shared Edition) Grants permission to manually synchronize images.	Write	repo *	-
			-	swr:TargetRegion
swr:repo:deleteAutoSyncRepoJob	(Shared Edition) Grants permission to delete an automatic image synchronization task.	Write	repo *	-
swr:repo:listAutoSyncRepoJobs	(Shared Edition) Grants permission to list automatic image synchronization tasks.	List	repo *	-
swr:repo:getSyncRepoJobInfo	(Shared Edition) Grants permission to query details about an image synchronization task.	Read	repo *	-
swr:repo:createTrigger	(Shared Edition) Grants permission to create a trigger.	Write	repo *	-
swr:repo:deleteTrigger	(Shared Edition) Grants permission to delete a trigger.	Write	repo *	-
swr:repo:listTriggers	(Shared Edition) Grants permission to list triggers.	List	repo *	-
swr:repo:getTrigger	(Shared Edition) Grants permission to query details about a trigger.	Read	repo *	-
swr:repo:updateTrigger	(Shared Edition) Grants permission to update a trigger.	Write	repo *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repo:createRetention	(Shared Edition) Grants permission to create an image retention policy.	Write	repo *	-
swr:repo:deleteRetention	(Shared Edition) Grants permission to delete an image retention policy.	Write	repo *	-
swr:repo:listRetentionHistories	(Shared Edition) Grants permission to list image retention records.	List	repo *	-
swr:repo:listRetentions	(Shared Edition) Grants permission to list image retention policies.	List	repo *	-
swr:repo:getRetention	(Shared Edition) Grants permission to query details about an image retention policy record.	Read	repo *	-
swr:repo:updateRetention	(Shared Edition) Grants permission to modify an image retention policy.	Write	repo *	-
swr::createLoginSecret	(Shared Edition) Grants permission to generate a temporary login command.	Write	-	-
swr::listQuotas	(Shared Edition) Grants permission to list quotas.	List	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr::getDomainOverview	(Shared Edition) Grants permission to query brief resource information of a tenant.	Read	-	-
swr::getDomainResourceReports	(Shared Edition) Grants permission to query resource statistics of a tenant.	Read	-	-
swr:namespace:multipartUpload	(Shared Edition) Grants permission to upload an image in multipart mode.	Write	namespace *	-
swr:namespace:createNamespaceAccess	(Shared Edition) Grants permission to create an organization permission.	Permission_management	namespace *	-
swr:namespace:deleteNamespaceAccess	(Shared Edition) Grants permission to delete an organization permission.	Permission_management	namespace *	-
swr:namespace:getNamespaceAccess	(Shared Edition) Grants permission to query details about an organization permission.	Read	namespace *	-
swr:namespace:updateNamespaceAccess	(Shared Edition) Grants permission to update an organization permission.	Permission_management	namespace *	-
swr:repo:createRepoAccess	(Shared Edition) Grants permission to create an image permission.	Permission_management	repo *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repo:deleteRepoAccess	(Shared Edition) Grants permission to delete an image permission.	Permission_management	repo *	-
swr:repo:getRepoAccess	(Shared Edition) Grants permission to query details about an image permission.	Read	repo *	-
swr:repo:updateRepoAccess	(Shared Edition) Grants permission to update an image permission.	Permission_management	repo *	-
swr:repo:upload	(Shared Edition) Grants permission to upload an image.	Write	repo *	-
swr:repo:download	(Shared Edition) Grants permission to download an image.	Read	repo *	-
swr:repository:createImmutableRule	(Enterprise Edition) Grants permission to create an immutability rule.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteImmutableRule	(Enterprise Edition) Grants permission to delete an immutability rule.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listImmutableRules	(Enterprise Edition) Grants permission to list immutability rules.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateImmutableRule	(Enterprise Edition) Grants permission to modify an immutability rule.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:listArtifacts	(Enterprise Edition) Grants permission to list artifacts.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getArtifact	(Enterprise Edition) Grants permission to query details about an artifact.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteArtifact	(Enterprise Edition) Grants permission to delete an artifact.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listAccessories	(Enterprise Edition) Grants permission to list artifact accessories.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getArtifactAddition	(Enterprise Edition) Grants permission to query additional information about an artifact.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getConfigurations	(Enterprise Edition) Grants permission to query specifications of an instance.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateConfigurations	(Enterprise Edition) Grants permission to update specifications of an instance.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listResourceInstances	(Enterprise Edition) Grants permission to list instances.	List	instance *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:TagKeys • g:RequestTag/<tag-key>
swr:instance:getResourceInstances-Count	(Enterprise Edition) Grants permission to query the number of instances.	Read	instance *	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
swr:instance:createResourceTags	(Enterprise Edition) Grants permission to batch create a resource tag.	Tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
swr:instance:deleteResourceTags	(Enterprise Edition) Grants permission to batch delete a resource tag.	Tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
swr:instance:getProjectTags	(Enterprise Edition) Grants permission to query project tags.	Read	-	-
swr:instance:getResourceTags	(Enterprise Edition) Grants permission to query resource tags.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:create	(Enterprise Edition) Grants permission to create an instance.	Write	instance *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • **swr:VpcId** • **swr:SubnetId** • **swr:EnableObsEncrypt**
swr:instance:list	(Enterprise Edition) Grants permission to list instances.	List	instance *	-
swr:instance:get	(Enterprise Edition) Grants permission to query details about an instance.	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
swr:instance:delete	(Enterprise Edition) Grants permission to delete an instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
swr:instance:getAuditLogs	(Enterprise Edition) Grants permission to query audit logs of an instance.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getStatistics	(Enterprise Edition) Grants permission to query statistics on an instance.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listJobs	(Enterprise Edition) Grants permission to list tasks.	List	instance *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:instance:getJobs	(Enterprise Edition) Grants permission to query details about a task.	Read	instance *	-
swr:instance:deleteJob	(Enterprise Edition) Grants permission to delete a task.	Write	instance *	-
swr:repository:createNamespace	(Enterprise Edition) Grants permission to create a namespace (an organization).	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	swr:EnablePublicNameSpace
swr:repository:listNamespaces	(Enterprise Edition) Grants permission to list namespaces (organizations).	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getNamespace	(Enterprise Edition) Grants permission to query details about a namespace (an organization).	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateNamespace	(Enterprise Edition) Grants permission to modify a namespace (an organization).	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	swr:EnablePublicNameSpace
swr:repository:deleteNamespace	(Enterprise Edition) Grants permission to delete a namespace (an organization).	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:listRepositories	(Enterprise Edition) Grants permission to list artifact repositories.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getRepository	(Enterprise Edition) Grants permission to query details about an artifact repository.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateRepository	(Enterprise Edition) Grants permission to modify an artifact repository.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteRepository	(Enterprise Edition) Grants permission to delete an artifact repository.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listTags	(Enterprise Edition) Grants permission to list artifact tags.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getTag	(Enterprise Edition) Grants permission to query details about an artifact tag.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteTag	(Enterprise Edition) Grants permission to delete an artifact tag.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:getTagAddition	(Enterprise Edition) Grants permission to query additional information about an artifact tag.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createRetentionPolicy	(Enterprise Edition) Grants permission to create a tag retention policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listRetentionPolicies	(Enterprise Edition) Grants permission to list tag retention policies.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getRetentionPolicy	(Enterprise Edition) Grants permission to query details about a tag retention policy.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateRetentionPolicy	(Enterprise Edition) Grants permission to modify a tag retention policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteRetentionPolicy	(Enterprise Edition) Grants permission to delete a tag retention policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:executeRetentionPolicy	(Enterprise Edition) Grants permission to execute tag retention policies.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listRetentionPolicyExecutions	(Enterprise Edition) Grants permission to list tag retention records.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:listRetentionPolicyExecTasks	(Enterprise Edition) Grants permission to list tag retention tasks.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listRetentionPolicyExecSubTasks	(Enterprise Edition) Grants permission to list tag retention subtasks.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createWebhook	(Enterprise Edition) Grants permission to create a trigger.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listWebhooks	(Enterprise Edition) Grants permission to list triggers.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getWebhook	(Enterprise Edition) Grants permission to query details about a trigger.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateWebhook	(Enterprise Edition) Grants permission to modify a trigger.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteWebhook	(Enterprise Edition) Grants permission to delete a trigger.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listWebhookJobs	(Enterprise Edition) Grants permission to list triggering records.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:instance:createRegistry	(Enterprise Edition) Grants permission to create a destination registry.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listRegistries	(Enterprise Edition) Grants permission to list destination registries.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getRegistry	(Enterprise Edition) Grants permission to query details about a destination registry.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateRegistry	(Enterprise Edition) Grants permission to modify a destination registry.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteRegistry	(Enterprise Edition) Grants permission to delete a destination repository.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createReplicationPolicy	(Enterprise Edition) Grants permission to create a replication policy.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listReplicationPolicies	(Enterprise Edition) Grants permission to list replication policies.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:instance:getReplicationPolicy	(Enterprise Edition) Grants permission to query details about a replication policy.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateReplicationPolicy	(Enterprise Edition) Grants permission to modify a replication policy.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteReplicationPolicy	(Enterprise Edition) Grants permission to delete a replication policy.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:executeReplicationPolicy	(Enterprise Edition) Grants permission to execute replication policies.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:stopReplicationPolicyExecution	(Enterprise Edition) Grants permission to stop replication tasks.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listReplicationPolicyExecutions	(Enterprise Edition) Grants permission to list replication records.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listReplicationPolicyExecTasks	(Enterprise Edition) Grants permission to list replication tasks.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listReplicationPolicyExecSubTasks	(Enterprise Edition) Grants permission to list replication subtasks.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:createSignPolicy	(Enterprise Edition) Grants permission to create a sign policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listSignPolicies	(Enterprise Edition) Grants permission to list sign policies.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getSignPolicy	(Enterprise Edition) Grants permission to query details about a sign policy.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateSignPolicy	(Enterprise Edition) Grants permission to modify a sign policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteSignPolicy	(Enterprise Edition) Grants permission to delete a sign policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:executeSignPolicy	(Enterprise Edition) Grants permission to execute sign policies.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listSignPolicyExecu-tions	(Enterprise Edition) Grants permission to list signing records.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listSignPolicyExecTasks	(Enterprise Edition) Grants permission to list signing tasks.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:listSignPolicyExecSubTasks	(Enterprise Edition) Grants permission to list signing subtasks.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createScanPolicy	(Enterprise Edition) Grants permission to create a scan policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listScanPolicies	(Enterprise Edition) Grants permission to list scan policies.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getScanPolicy	(Enterprise Edition) Grants permission to query details about a scan policy.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateScanPolicy	(Enterprise Edition) Grants permission to modify a scan policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteScanPolicy	(Enterprise Edition) Grants permission to delete a scan policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:executeScanPolicy	(Enterprise Edition) Grants permission to execute scan policies.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listScanPolicyExecu-tions	(Enterprise Edition) Grants permission to list scanning records.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:listScanPolicyExecTasks	(Enterprise Edition) Grants permission to list scanning tasks.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:createBlockPolicy	(Enterprise Edition) Grants permission to create a block policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listBlockPolicies	(Enterprise Edition) Grants permission to list block policies.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:getBlockPolicy	(Enterprise Edition) Grants permission to query details about a block policy.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:updateBlockPolicy	(Enterprise Edition) Grants permission to modify a block policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:deleteBlockPolicy	(Enterprise Edition) Grants permission to delete a block policy.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:listBlockPolicyRecords	(Enterprise Edition) Grants permission to list blocking records.	List	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateEndpointPolicy	(Enterprise Edition) Grants permission to update the whitelist for public network access.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:instance:updateEndpointPolicyStatus	(Enterprise Edition) Grants permission to update the whitelist status for public network access.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:getEndpointPolicy	(Enterprise Edition) Grants permission to query the whitelist for public network access.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createInternalEndpoint	(Enterprise Edition) Grants permission to allow a connection from the intranet.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• **swr:VpcId** • **swr:SubnetId**
swr:instance:getInternalEndpoint	(Enterprise Edition) Grants permission to query details about an allowed connection from the intranet.	Read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteInternalEndpoint	(Enterprise Edition) Grants permission to deny a connection from the intranet.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listInternalEndpoints	(Enterprise Edition) Grants permission to list allowed connections from the intranet.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:repository:uploadArtifact	(Enterprise Edition) Grants permission to upload artifacts.	Write	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:repository:downloadArtifact	(Enterprise Edition) Grants permission to download artifacts.	Read	repository *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createTempCredential	(Enterprise Edition) Grants permission to create a temporary access credential.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:createLTCredential	(Enterprise Edition) Grants permission to create a long-term access credential.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateLTCredential	(Enterprise Edition) Grants permission to enable or disable long-term access credentials.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listLTCredentials	(Enterprise Edition) Grants permission to list long-term access credentials.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteLTCredential	(Enterprise Edition) Grants permission to delete a long-term access credential.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
swr:instance:addDomainName	(Enterprise Edition) Grants permission to add a domain name.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:deleteDomainName	(Enterprise Edition) Grants permission to delete a domain name.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:updateDomainName	(Enterprise Edition) Grants permission to update a domain name.	Write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
swr:instance:listDomainNames	(Enterprise Edition) Grants permission to list domain names.	List	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Each API of SWR usually supports one or more actions. **Table 5-76** lists the supported actions and dependencies.

Table 5-76 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	-

API	Action	Dependencies
POST /v2/manage/namespaces/{namespace}/repos	swr:repo:createRepo	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:deleteRepo	-
GET /v2/manage/repos	swr:repo:listRepos	-
GET /v2/manage/shared-repositories	swr:repo:listSharedRepos	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:getRepo	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}	swr:repo:updateRepo	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/tags/{tag}	swr:repo:deleteRepoTag	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/tags	swr:repo:createRepoTag	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/tags	swr:repo:listRepoTags	-
POST /v2/manage/namespaces/{namespace}/repositories/{repository}/access-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
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	• swr::createLoginSecret • swr:repo:download • swr:repo:upload
POST /v2/manage/namespaces/{namespace}/repos/{repository}/sync_images	swr:repo:createManualSyncRepoJob	• swr::createLoginSecret • swr:repo:download • swr:repo:upload
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	-
DELETE /v2/manage/namespaces/{namespace}/repos/{repository}/triggers/{trigger}	swr:repo:deleteTrigger	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/triggers	swr:repo:listTriggers	-

API	Action	Dependencies
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	-
GET /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:getRetention	-
PATCH /v2/manage/namespaces/{namespace}/repos/{repository}/retentions/{retention_id}	swr:repo:updateRetention	-

API	Action	Dependencies
POST /v2/manage/utils/secret	swr::createLoginSecret	-
GET /v2/manage/projects/{project_id}/quotas	swr::listQuotas	-
GET /v2/manage/overview	swr::getDomainOverview	-
GET /v2/manage/reports/{resource_type}/{frequency}	swr::getDomainResourceReports	-
POST /v2/manage/namespaces/{namespace}/access	swr:namespace:createNamespaceAccess	-
DELETE /v2/manage/namespaces/{namespace}/access	swr:namespace:deleteNamespaceAccess	-
GET /v2/manage/namespaces/{namespace}/access	swr:namespace:getNamespaceAccess	-
PATCH /v2/manage/namespaces/{namespace}/access	swr:namespace:updateNamespaceAccess	-
POST /v2/manage/namespaces/{namespace}/repos/{repository}/access	swr:repo:createRepoAccess	-
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	-

CAUTION

In addition to the fine-grained authentication provided by IAM, you can also use the authentication provided by SWR. If an action is allowed by SWR authentication and it is not denied on IAM, this action will be allowed.

The actions **swr::createLoginSecret**, **swr:namespace:listNamespaces**, **swr:repo:listRepos**, **swr::getDomainOverview**, **swr::getDomainResourceReports**, **swr:repo:listSharedRepos** are allowed by SWR authentication by default. So, to block users from performing these actions, you need to configure deny policies for them in IAM.

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-77**, 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 SWR.

Table 5-77 Resource types supported by SWR

Resource Type	URN
repo	swr:<region>:<account-id>:repo:<namespace-name>/<repo-name>
repository	swr:<region>:<account-id>:repository:<instance-name>/<repository-path>
instance	swr:<region>:<account-id>:instance:<instance-name>
namespace	swr:<region>:<account-id>:namespace:<namespace-name>

Conditions

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, 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, **swr:**) only apply to operations of the SWR service. For details, see **Table 5-78**.
  - 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.

The following table lists the condition keys that you can define in SCPs for SWR. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-78 Service-specific condition keys supported by SWR

Condition Key	Value Type	Single-valued/ Multivalued	Description
swr:TargetOrgPath	string	Single-valued	Controls permissions of target sharing accounts based on their organization paths.
swr:TargetOrgId	string	Single-valued	Controls permissions of target sharing accounts based on their organization IDs.
swr:TargetAccountId	string	Single-valued	Controls permissions of target sharing accounts based on their IDs.
swr:VpcId	string	Single-valued	Controls permissions based on VPC IDs.
swr:SubnetId	string	Single-valued	Controls permissions based on subnet IDs.
swr:EnablePublicNameSpace	boolean	Single-valued	Controls whether public organizations can be created in SWR Enterprise Edition.

Condition Key	Value Type	Single-valued/ Multivalued	Description
swr:EnableObsEncrypt	boolean	Single-valued	Controls whether buckets must be encrypted in SWR Enterprise Edition.
swr:AllowPublicAccess	boolean	Single-valued	Controls whether images can be public.
swr:TargetRegion	string	Single-valued	Controls permissions based on destination regions.

5.10.5 Analytics

5.10.5.1 Data Lake Insight (DLI)

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.

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

- For 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 DLI, 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 DLI, see **Conditions**.

The following table lists the actions that you can define in custom SCP statements for DLI.

Table 5-79 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 *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:queue:create	Grants the permission to create queues.	write	queue *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dli:queue:get	Grants the permission to query queue details.	read	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:update	Grants the permission to update queues.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:delete	Grants the permission to delete queues.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:scale	Grants the permission to scale out/in a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dli:queue:checkConnection	Grants the permission to test the connectivity of an address.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:getConnection	Grants the permission to query connectivity results.	read	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:listPlans	Grants the permission to list scheduled scaling plans of a queue.	list	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:createPlan	Grants the permission to create scheduled scaling plans for a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:deletePlan	Grants the permission to delete scheduled scaling plans from a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:updatePlan	Grants the permission to update scheduled scaling plans for a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:createProperty	Grants the permission to create configurations for a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:listProperties	Grants the permission to list queue configurations.	list	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dli:queue:updateProperty	Grants the permission to update configurations for a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:deleteProperty	Grants the permission to delete configurations from a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:jobs:list	Grants the permission to list jobs.	list	jobs *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:queue:submitJob	Grants the permission to submit jobs on a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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 *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:insertInto	Grants the permission to insert table data.	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:queue:cancelJob	Grants the permission to cancel jobs on a queue.	write	queue *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

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 *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:database:create	Grants the permission to create databases.	write	database *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dli:database:update	Grants the permission to update databases.	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:database:delete	Grants the permission to delete databases.	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:database:displayAllTables	Grant the permission to display all tables in a database.	list	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:database:createTable	Grants the permission to create tables in a database.	write	database *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dli:table:update	Grants the permission to update tables.	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:describe	Grants the permission to display the table structure.	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:delete	Grants the permission to delete tables.	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:showPartitions	Grants the permission to display all partitions of a table.	read	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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 *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
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 *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
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 *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys

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:elasticresourcepool:resourceManagement	Grants the permission to manage resources to an elastic resource pool.	write	elasticresource-pool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:elasticresourcepool:list	Grants the permission to list elastic resource pools.	list	elasticresource-pool *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:elasticresourcepool:create	Grants the permission to create elastic resource pools.	write	elasticresource-pool *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dli:elasticresourcepool:update	Grants the permission to update elastic resource pools.	write	elasticresource-pool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:elasticresourcepool:delete	Grants the permission to delete elastic resource pools.	write	elasticresource-pool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dli:elasticresourcepool:scale	Grants the permission to scale out/in an elastic resource pool.	list	elasticresource-pool *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
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	-	• g:RequestTag/<tag-key> • g:TagKeys
dli:connection:create	Grants the permission to create basic datasource connections.	write	-	• g:RequestTag/<tag-key> • g:TagKeys
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 *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dli:edsconnection:create	Grants the permission to create enhanced datasource connections.	write	edsconnection *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • dli:VpcId
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 *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dli:table:insertOverwriteTable	Grants the permission to overwrite data to a table.	write	table *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

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	-	• g:RequestTag/<tag-key> • g:TagKeys
dli::unTagResource	Grants the permission to delete tags.	tagging	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			resource	g:ResourceTag/<tag-key>
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			elasticresource-pool	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			edsconnection	g:ResourceTag/<tag-key>
			jobs	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dli::listTagsForResource	Grants the permission to query the tags of a specified resource.	list	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			resource	g:ResourceTag/<tag-key>
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			elasticresource-pool	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			edsconnection	g:ResourceTag/<tag-key>
			jobs	g:ResourceTag/<tag-key>
dli::createDownloader	Grants the permission to create download tasks.	write	-	-
dli::tagResource	Creates resource tags.	tagging	queue	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			resource	g:ResourceTag/<tag-key>
			database	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			elasticresource-pool	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			edsconnection	g:ResourceTag/<tag-key>
			jobs	g:ResourceTag/<tag-key>
dli:jobs:check	Verifies if jobs exist.	read	-	-
dli:jobs:import	Imports jobs.	write	jobs	-
dli:template:check	Verifies if templates exist.	read	-	-

Each API of DLI usually supports one or more actions. **Table 5-80** lists the actions and dependencies supported by DLI APIs.

Table 5-80 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	-
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	-

API	Action	Dependency
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	-
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	-

API	Action	Dependency
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	-
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	-

API	Action	Dependency
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:import	-
POST /v3/{project_id}/streaming/jobs/{job_id}/gen-graph	dli:jobs:get	-
GET /v1.0/{project_id}/streaming/job-templates	dli:template:list	-
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	-

API	Action	Dependency
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	-
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	-

API	Action	Dependency
GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues	dli:elasticresourcepool:resourceManagement	-
POST /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues	dli:elasticresourcepool:resourceManagement	• dli:queue:create • dli:queue:delete
PUT /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/queues/{queue_name}	dli:elasticresourcepool:resourceManagement	-
GET /v3/{project_id}/elastic-resource-pools/{elastic_resource_pool_name}/scale-records	dli:elasticresourcepool:scale	-
POST /v3/{project_id}/orders/elastic-resource-pools	dli:elasticresourcepool:create	-
POST /v3/{project_id}/orders/elastic-resource-pools/specification-change	dli:elasticresourcepool: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	-
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	-

API	Action	Dependency
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	-
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::listResourcesByTag	-

API	Action	Dependency
POST /v3/{project_id}/{resource_type}/resource-instances/count	dli::listResourcesByTag	-
POST /v3/{project_id}/{resource_type}/{resource_id}/tags/delete	dli::unTagResource	-
GET /v3/{project_id}/{resource_type}/{resource_id}/tags	dli::listTagsForResource	-

Table 5-81 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	-
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	-

API	Action	Dependency
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 SCP applies to. If you specify a resource type for any action in **Table 5-82**, 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 DLI.

Table 5-82 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>

Resource Type	URN
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>:elasticresource-pool:<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 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 as the prefix, for example, **dli:**) apply only to DLI operations. For details, see **Table 5-83**.
  - 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 SCP 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 DLI. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-83 Service-specific condition keys supported by DLI

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
dli:VpcId	string	Single-valued	Filters access permissions by VPC ID.

5.10.5.2 DataArts Studio

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 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.

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 DataArts Studio, see **Resources**.

- **Condition Key** 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 DataArts Studio, see **Conditions**.

The following table lists the actions that you can define in SCP statements for DataArts Studio.

NOTE

Due to API restrictions, if the resource type is specified for an SCP, 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 an SCP, you must exclude such operations. Instead, you can only configure SCP statements without specified resources or with global resources for such operations, and use multiple SCP statements to grant permissions to users. SCP statements 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 5-84 Actions supported by DataArts Studio

Action	Description	Access Level	Resource Type (*: required)	Condition Key
DataArtsStudio:workspace:list	Grants the permission to query all workspaces.	list	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:create	Grants the permission to create a workspace.	write	workspace *	-
			instance *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
DataArtsStudio:workspace:get	Grants the permission to query workspace information.	read	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:frozen	Grants the permission to freeze a workspace.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:unfrozen	Grants the permissions to unfreeze a workspace.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:update	Grants the permission to update a workspace.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:list	Grants the permission to query all instances.	list	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:create	Grants the permission to create an instance.	write	instance *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:RequestTag/<tag-key> • g:TagKeys
DataArtsStudio:instance:get	Grants the permission to query an instance.	read	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:resize	Grants the permission to change instance specifications.	write	instance *	g:ResourceTag/<tag-key>
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 *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:getAgency	Grants the permission to query an agency.	read	-	-
DataArtsStudio:instance:createAgency	Grants the permission to create an agency.	write	-	-
DataArtsStudio:instance:delete	Grants the permission to delete an instance.	write	instance *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
DataArtsStudio:instance:migrateBusinessModel	Grants the permission to change the business model of an instance.	write	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:operate	Grants the permission to operate the resources of an instance.	write	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:operate	Grants the permission to operate the resources in a workspace.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:createRole	Grants the permission to create a custom role.	write	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:listRoles	Grants the permission to query custom roles.	list	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:getRoleType	Grants the permission to query the type of a custom role.	read	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:getRole	Grants the permission to query a custom role.	read	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:updateRole	Grants the permission to update a custom role.	write	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:deleteRole	Grants the permission to delete a custom role.	write	instance *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
DataArtsStudio:instance:tagResource	Grants the permission to add an instance tag.	write	instance *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
DataArtsStudio:instance:unTagResource	Grants the permission to delete an instance tag.	write	instance *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
DataArtsStudio:instance:listIncrementalPackages	Grants the permission to query all incremental packages.	list	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:createIncrementalPackage	Grants the permission to create an incremental package for a workspace.	write	workspace *	• g:ResourceTag/<tag-key> • DataArtsStudio:EnablePublicAccess
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:tagResource	Grants the permission to add a tag to a workspace.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
DataArtsStudio:workspace:unTagResource	Grants the permission to delete a tag from a workspace.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
DataArtsStudio:instance:createIncrementalPackage	Grants the permission to create an incremental package for an instance.	write	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:listTags	Grants the permission to query the tags of all instances.	list	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:listTags	Grants the permission to query the tags of all workspaces.	list	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:listTagsForResource	Grants the permission to query the tags of an instance.	list	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:listTagsForResource	Grants the permission to query the tags of a workspace.	list	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:updateDataServiceApiQuota	Grants the permission to update the DataArts DataService API quota of a workspace.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>
DataArtsStudio:workspace:executeDataServiceInstanceAction	Grants the permission to run commands to perform operations on DataArts DataService clusters.	write	workspace *	g:ResourceTag/<tag-key>
			instance *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
DataArtsStudio:instance:configureDataSecurityAdministrator	Grants the permission to configure the data security administrator.	write	instance *	g:ResourceTag/<tag-key>
DataArtsStudio:instance:listResourcesByTag	Grants the permission to filter instances by tag.	list	instance *	-
			-	g:TagKeys
DataArtsStudio:workspace:listResourcesByTag	Grants the permission to filter workspaces by tag.	list	workspace *	-
			instance *	-
			-	g:TagKeys

Each API of DataArts Studio usually supports one or more actions. **Table 5-85** lists the actions and dependencies supported by DataArts Studio APIs.

Table 5-85 Actions and dependencies supported by DataArts Studio APIs

API	Action	Dependencies
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	-

API	Action	Dependencies
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 SCP applies to. If you specify a resource type for any action in **Table 5-86**, 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 an SCP for DataArts Studio.

Table 5-86 Resource types supported by DataArts Studio

Resource Type	URN
workspace	DataArtsStudio:<region>:<account-id>:workspace:<instance-id>/<workspace-id>
instance	DataArtsStudio:<region>:<account-id>:instance:<instance-id>

Conditions

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 for an SCP 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 as the prefix, for example, **DataArtsStudio:**) apply only to DataArts Studio operations. For details, see **Table 5-87**.
  - 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.

- An operator, a condition key, and a condition value together constitute a complete condition statement. An SCP becomes in effect only when its request conditions are met. For supported operators, see Operators.

The following table lists the condition keys that you can define in an SCP for DataArts Studio. You can include these condition keys to specify conditions for when your SCP statement is in effect.

Table 5-87 Service-specific condition keys supported by DataArts Studio

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
DataArtsStudio:EnablePublicAccess	boolean	Single-valued	Whether the service is accessible over the Internet

5.10.5.3 GaussDB(DWS)

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 GaussDB(DWS), see **Resource Type**.

- 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 condition keys defined by GaussDB(DWS), see **Conditions**.

The following table lists the actions that you can define in SCP statements for GaussDB(DWS).

Table 5-88 Actions supported by GaussDB(DWS)

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:list	Grants the permission to query the cluster list.	list	-	-
dws:cluster:getDetail	Grants the permission to view cluster details.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:create	Grants the permission to create a GaussDB(DWS) cluster.	write	-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dws:cluster:delete	Grants the permission to delete a GaussDB(DWS) cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:scaleIn	Grants the permission to scale in a GaussDB(DWS) cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listRing	Grants the permission to obtain the proper scale-in ring list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restore	Grants the permission to restore a snapshot to the original cluster.	write	cluster *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dws:cluster:scaleOut	Grants the permission to scale out a GaussDB(DWS) cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resize	Grants the permission to scale out and resize a GaussDB(DWS) cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:expandDisk	Grants the permission to expand the disk capacity of a GaussDB(DWS) cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restart	Grants the permission to restart a GaussDB(DWS) cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:resetPassword	Grants the permission to reset the password of a GaussDB(DWS) cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAuditLog	Grants the permission to view the audit log list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:setMaintainceWindow	Grants the permission to modify the maintenance time window.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchover	Grants the permission to restore a primary/standby cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:cancelReadonly	Grants the permission to remove the read-only status of a cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addCN	Grants the permission to add CNs to a cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listCN	Grants the permission to obtain the CN list of a cluster.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteCN	Grants the permission to delete CN nodes.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:redistribution	Grants the permission to redistribute cluster data.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createDataSource	Grants the permission to create MRS data sources.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateDataSource	Grants the permission to update MRS data sources.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteDataSource	Grants the permission to delete MRS data sources.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:alarm:listDetail	Grants the permission to query the alarm details list.	list	-	-
dws:alarm:report	Grants the permission to report alarms.	write	-	-
dws:event:createSpec	Grants the permission to create event configurations.	write	-	-
dws:event:deleteSpec	Grants the permission to delete event configurations.	write	-	-
dws:event:report	Grants the permission to report events.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:createConnection	Grants the permission to create a GaussDB(DWS) cluster connection.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteConnection	Grants the permission to delete GaussDB(DWS) cluster connections.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateConnection	Grants the permission to update GaussDB(DWS) cluster connections.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindEIP	Grants the permission to bind public IP addresses.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:unbindEIP	Grants the permission to unbind public IP addresses.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listELB	Grants the permission to obtain the ELB list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindELB	Grants the permission to bind ELBs.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:unbindELB	Grants the permission to unbind ELBs.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:createSnapshotPolicy	Grants the permission to set automated snapshot policies.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshotStatistics	Grants the permission to query the snapshot space capacity.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshot	Grants the permission to view the cluster snapshot list.	list	cluster	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSnapshotDetail	Grants the permission to view cluster snapshot details.	list	cluster	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createSnapshot	Grants the permission to create snapshots using APIs.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteSnapshotPolicy	Grants the permission to delete snapshot policies.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshotPolicy	Grants the permission to query snapshot policies.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:copySnapshot	Grants the permission to replicate snapshots.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteSnapshot	Grants the permission to delete snapshots.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:restoreSnapshot	Grants the permission to restore snapshots.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteDisasterRecovery	Grants the permission to delete DR tasks.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createDisasterRecovery	Grants the permission to create DR tasks.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restoreDisaster	Grants the permission to restore DR tasks.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws::listTagsForProject	Grants the permission to query the tag list in the project.	list	-	-
dws:cluster:listConfig	Grants the permission to view cluster configuration parameters.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:service:listSpec	Grants the permission to view the service specification list.	list	-	-
dws:cluster:listDataSource	Grants the permission to view cluster data sources.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:service:listJobDetail	Grants the permission to view task progress details.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:service:listStatistics	Grants permission to view available resources.	list	-	-
dws:service:listQuotas	Grants the permission to view user quotas.	list	-	-
dws:cluster:updateConfig	Grants the permission to update cluster configuration parameters.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:service:listAZ	Grants the permission to view the service AZ list.	list	-	-
dws:service:listDssPools	Grants the permission to view the storage pool list.	list	-	-
dws:service:listEps	Grants the permission to view the EPS list.	list	-	-
dws:service:authorize	Grant the permission to obtain user authorization.	write	-	-
dws:service:checkAuthorize	Grant the permission to check user authorization.	read	-	-
dws::updateTag	Grants the permission to update tags.	tagging	cluster *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getSnapshotPolicy	Grants the permission to view snapshot policies.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindOrUnbindELB	Grants the permission to bind or unbind ELBs.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindOrUnbindEIP	Grants the permission to bind or unbind EIPs.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteNode	Grants the permission to delete nodes.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listConnection	Grants the permission to query the GaussDB(DWS) cluster connection list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkConnection	Grants the permission to check the GaussDB(DWS) cluster connections.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDN	Grants the permission to obtain the DN list of a cluster.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listBucket	Grants the permission to obtain the bucket list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listScaleInNode	Grants the permission to obtain the list of nodes to be deleted.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listFlavorForResize	Grants the permission to query the list of flavors that can be modified.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listFlavorForRestore	Grants the permission to query the list of flavors that can be restored.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws::countResourceByTag	Grants the permission to query clusters using tags.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateSnapshotPolicy	Grants the permission to update snapshot policies.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws::listResourceByTag	Grants the permission to query clusters by tag.	list	cluster *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dws:cluster:assessRisk	Grants the permission to evaluate the risk of resizing.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkRestoreTable	Grants the permission to check the restored table.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:checkSupportFineGrainedBackup	Grants the permission to check whether a cluster supports fine-grained backup.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:configureNetwork	Grants the permission to configure the cluster network.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:expandWithExistedNodes	Grants the permission to scale out a cluster from an idle node.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getAntiAffinity	Grants the permission to query the anti-affinity status.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getCnCount	Grants the permission to query the number of CNs in a cluster.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getCredential	Grants the permission to obtain the JDBC connection credential of a cluster.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDiskExpandScope	Grants the permission to obtain the disk scale-out scope.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getEncryptInfo	Grants the permission to view cluster encryption information.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listHistoryConfig	Grants the permission to query parameter modification history.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getHistoryConfigDetail	Grants the permission to query parameter modification history details.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getInstanceDetail	Grants the permission to view instance details.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getProcessTopo	Grants the permission to query the cluster node process topology.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getRedistribution	Grants the permission to query redistribution details.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getRestoreDatabase	Grants the permission to restore databases.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getRoachConfig	Grants the permission to obtain **roach** parameter configurations.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSnapshotEncryptInfo	Grants the permission to view snapshot encryption information.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getSnapshotStorage	Grants the permission to query the snapshot capacity usage.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getTaskDetail	Grants the permission to query cluster task details.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getVolumeInfo	Grants the permission to query disk information.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listNode	Grants the permission to query the node list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSchema	Grants the permission to obtain the user structure list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listTable	Grants the permission to obtain the user list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDatabase	Grants the permission to obtain the database list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:recoverRedistribution	Grants the permission to restore redistribution.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resizeFlavor	Grants the permission to change specifications.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:resizeRetry	Grants the permission to retry failed resize attempts.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restoreTable	Grants the permission to restore tables.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:retryELBSwitch	Grants the permission to retry an ELB switchover task.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listRingForScaleIn	Grants the permission to obtain the scale-in ring list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopSnapshot	Grants the permission to stop snapshots.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:suspendRedistribution	Grants the permission to suspend redistribution.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateInstanceAliasName	Grants the permission to update the node alias.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateRoachConfig	Grants the permission to update **roach** parameter configurations.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateScheduleConfig	Grants the permission to update scheduling configurations.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:service:getClusterSum	Grants the permission to query the number of clusters.	read	-	-
dws:service:getResourceStatistics	Grants the permission to query resource statistics.	read	-	-
dws:service:getStorageStatistics	Grants the permission to query storage statistics.	read	-	-
dws:cluster:listDisasterRecovery	Grants the permission to query the DR task list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkDisasterRecovery-Name	Grants the permission to check DR task names.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateDisasterRecover-yConfig	Grants the permission to update DR configurations.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addOperationalTask	Grants the permission to add scheduling tasks.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:bindManageIp	Grants the permission to bind management plane IP addresses.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:checkAccessLts	Grants the permission to check whether LTS is normal.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:checkLogicalClusterData	Grants the permission to check whether a logical cluster has the service data operation permission.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:closeAccessLts	Grants the permission to disable cloud service logs.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createLogicalCluster	Grants the permission to create a logical cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createApplicationForDM	Grants the permission to add jobs and tasks during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createClusterForDM	Grants the permission to create clusters during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createConnectionForDM	Grants the permission to add connections during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createMappingForDM	Grants the permission to add mappings during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteApplicationForDM	Grants the permission to delete jobs and tasks during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:deleteClusterForDM	Grants the permission to delete clusters during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteConnectionForDM	Grants the permission to delete connections during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteMappingForDM	Grants the permission to delete mappings during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:dialsConnectionForDM	Grants the permission to probe connection activity during data migration.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getApplicationForDM	Grants the permission to query job and task details during data migration.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listApplicationConfigForDM	Grants the permission to configure data migration job and task parameters.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listApplicationForDM	Grants the permission to query all jobs in a cluster during data migration.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterForDM	Grants the permission to query cluster details during data migration.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listClusterForDM	Grants the permission to query the cluster list during data migration.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listConfigurationTemplateForDM	Grants the permission to query parameter templates during data migration.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getConnectionForDM	Grants the permission to query connection details during data migration.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listConnectionForDM	Grants the permission to query all connections during data migration.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDependApplicationForDM	Grants the permission to query all dependent jobs during data migration.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMappingForDM	Grants the permission to query mapping details during data migration.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listMappingForDM	Grants the permission to query all mappings during data migration.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listProductForDM	Grants the permission to query product information in GDS-Kafka.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:updateConnectionForDM	Grants the permission to modify the specified connection during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateMappingForDM	Grants the permission to modify the specified mapping during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:startApplicationForDM	Grants the permission to start jobs and tasks during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopApplicationForDM	Grants the permission to stop jobs and tasks during data migration.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteCrossRegionSnapshotPolicy	Grants the permission to delete cross-region backup configurations.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteLogicalCluster	Grants the permission to delete a logical cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteOperationalTask	Grants the permission to delete scheduling tasks in the scheduler.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:operateDisasterRecovery	Grants permissions for DR operations, including starting, stopping, and switching over.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateLogicalCluster	Grants the permission to update a logical cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAllCrossRegionSnapshotConfig	Grants the permission to query all cross-region snapshot configurations.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDisasterRecoveryProject	Grants the permission to query available projects.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDisasterRecoveryRegion	Grants the permission to query available regions.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getLastOperationalTask	Grants the permission to query the operations of the last built tasks in the scheduler.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getLogicalClusterRings	Grants the permission to query the cluster ring information of a logical cluster.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getLogicalClusterVolume	Grants the permission to query disk information of a logical cluster.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getOperationalTaskConfig	Grants the permission to obtain the O&M task common configurations of the scheduler.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getOperationalTaskDetail	Grants the permission to obtain the O&M task details of the scheduler.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getOperationalTaskStatus	Grants permission to check the status of the scheduler.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSnapshotRegion	Grants permission to view the regions where cross-region snapshots are available.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getTargetAllCrossRegionSnapshotConfig	Grants the permission to query all cross-region snapshot configurations.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:initLogicalClusterSwitch	Grants the permission to enable and disable a logical cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAccessLts	Grants the permission to query the LTS list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listLogicalCluster	Grants the permission to query the logical cluster list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listLogicalClusterTask	Grants the permission to query task information of a logical cluster.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listOperationalTask	Grants the permission to obtain the O&M task list of the scheduler.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:openAccessLts	Grants the permission to enable cloud service logs.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:pauseOperationalTask	Allows the scheduler to suspend scheduling tasks.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDisasterRecoveryDetail	Grants the permission to query DR details.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:refreshOperationalTask	Allows remote refreshing of O&M tasks for the current cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:restartLogicalCluster	Grants the permission to restart a logical cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resumeOperationalTask	Grants the permission to resume scheduling tasks of the scheduler.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:setCrossRegionSnapshotPolicy	Grants the permission to configure cross-region backup.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:startOperationalTask	Grants the permission to enable the scheduler.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopOperationalTask	Grants the permission to disable the scheduler.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchLogicalCluster	Grants the permission to switch to a logical cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncCrossRegionBackup-ClusterInfo	Grants the permission to synchronize cross-region backup cluster information.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncCrossRegionBackup-Config	Grants the permission to synchronize cross-region snapshot configurations.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncCrossRegionBackupInfo	Grants the permission to synchronize cross-region snapshots.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:syncLogicalCluster	Grants the permission to synchronize data from the background in a logical cluster.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateOperationalTask-Config	Grants the permission to modify the O&M task common configurations of the scheduler.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:updateOperationalTask	Grants the permission to modify scheduling tasks of the scheduler.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addPlanForWLM	Grants the permission to add workload plans for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addPlanStageForWLM	Grants the permission to add workload plan stages for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addQueueForWLM	Grants the permission to add workload queues for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addQueueUserForWLM	Grants the permission to bind users to a workload queue for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePlanForWLM	Grants the permission to delete workload plans for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePlanStageForWLM	Grants the permission to delete workload plan stages for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:deleteQueueForWLM	Grants the permission to delete workload queues for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteQueueUserForWLM	Grants the permission to unbind users from a workload queue for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:exportPlanForWLM	Grants the permission to export workload plans for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPlanDetailForWLM	Grants the permission to query details about a workload plan for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPlanLogForWLM	Grants the permission to query workload plan logs for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPlanQueueForWLM	Grants the permission to query whether a queue is in a workload plan for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getPlanStageForWLM	Grants the permission to query workload plan stages for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueueForWLM	Grants the permission to obtain the workload queue list for workload management.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueueDetailForWLM	Grants the permission to obtain workload queues for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueueRuleForWLM	Grants the permission to obtain the exception rules of a workload queue for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:importPlanForWLM	Grants the permission to import workload plans for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listPlanQueueForWLM	Grants the permission to query available queues for all workload plans for workload management.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listPlanForWLM	Grants the permission to query workload plans for workload management.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueueUserForWLM	Grants the permission to obtain the bound users of a workload queue for workload management.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listUserForWLM	Grants the permission to obtain the list of users who are not bound to workload queues in the cluster for workload management.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterDBInfoForWLM	Grants the permission to query database information in a cluster for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listClusterPlanForWLM	Grants the permission to query all workload plans in a cluster for workload management.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterSchemaInfoForWLM	Grants the permission to query schema space information in a cluster for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getClusterVersionForWLM	Grants the permission to obtain the background database version in a cluster for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getFunctionStatusForWLM	Obtain the permission to enable or disable the workload function for workload management.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:setFunctionStatusForWLM	Grants the permission to set the status of the workload function switch for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:startPlanForWLM	Grants the permission to start a workload plan for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopPlanForWLM	Grants the permission to stop a workload plan for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchPlanStageForWLM	Grants the permission to switch workload stages for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:updatePlanStageForWLM	Grants the permission to modify workload plan stages for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateQueueBaseForWLM	Grants the permission to update workload queue basic information for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateQueueResourceForWLM	Grants the permission to update workload queue resource configuration for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateQueueRuleForWLM	Grants the permission to update workload queue exception rules for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateSchemaLimitForWLM	Grants the permission to update schema space limit for workload management.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorConfigForDMS	Grants the permission to query collection configuration or storage configuration in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:monitor:listClusterOverview	Grants the permission to check the cluster overview in DMS.	list	-	-
dws:cluster:listClusterInstanceForDMS	Grants the permission to obtain the cluster instance list in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDDLExamineDetailForDMS	Grants the permission to query review result details in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterDnStreamForDMS	Grants the permission to query DN data flow monitoring information in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listClusterAlarmRuleForDMS	Grants the permission to query the alarm rule list on the DMS tenant side.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterInstanceForDMS	Grants the permission to query instance information in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getHostNetMetricsForDMS	Grants the permission to query the network status in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getHistoryMetrics	Grants the permission to query historical monitoring data in DMS.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getMonitoringInfoForDMS	Grants the permission to query monitoring data in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listAlarmRuleForDMS	Grants the permission to query alarm rules by alarm ID on the DMS tenant side.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateCollectionItem-ForDMS	Grants the permission to update collection configuration in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:doDDLExamineActionForDMS	Grants the permission to manually trigger the review operation in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadDDLExamineDetailForDMS	Grants the permission to download DDL review details in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listInstanceDiskIOForDMS	Grants the permission to query disk I/Os in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:resetCollectionItemForDMS	Grants the permission to reset collection configuration in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueryRangeForDMS	Grants the permission to query time handles in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:monitor:getAlarmConfig	Grants the permission to query all clusters and alarm configurations on the DMS tenant side.	read	-	-
dws:cluster:switchoverCollectionI-temForDMS	Grants the permission to switch the collection switch in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getOSMetrics	Grants the permission to query GaussDB(DWS) hardware resource usage in DMS.	read	-	-
dws:cluster:listPerfDashboardForDMS	Allows the current user to access and query all performance monitoring panels in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:disableCollectionItem-ForDMS	Grants the permission to disable the collection function in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getAggregationOSMetrics	Grants the permission to query hardware resource usage of a GaussDB(DWS) cluster in DMS.	read	-	-
dws:cluster:terminateSessionForDMS	Grants the permission to terminate sessions in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getPerfDashboardDetail-ForDMS	Grants the permission to obtain panel information based on the panel ID in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:createAlarmRule	Grants the permission to add alarm rules on the DMS tenant side.	write	-	-
dws:cluster:enableCollectionItemForDMS	Grants the permission to enable the collection function in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listInstanceNetworkMetricsForDMS	Grants the permission to query NIC traffic of GaussDB(DWS) cluster nodes in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createPerfDashboardForDMS	Grants the permission to create user panels in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorMetricsForDMS	Grants the permission to obtain monitoring items on the home page in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createSQLProbeForDMS	Grants the permission to add SQL probes in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listInstanceIOStatusForDMS	Grants the permission to query disk I/O usage of GaussDB(DWS) cluster nodes in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorMetricsByDimensionForDMS	Grants the permission to obtain metrics by dimension in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateStorageConfigForDMS	Grants the permission to update storage configuration in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:updateAlarmRule	Grants the permission to modify alarm rules on the DMS tenant side.	write	-	-
dws:cluster:getInstanceIOAggResultForDMS	Grants the permission to query disk I/O aggregation usage of each node in a GaussDB(DWS) cluster in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updatePerfDashboardForDMS	Grants the permission to modify user panels in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorHistoryMetricsCost	Grants the permission to query historical queue consumption in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:monitor:deleteAlarmRule	Grants the permission to delete rules on the DMS tenant side.	write	-	-
dws:cluster:updateSQLProbeForDMS	Grants the permission to modify SQL probes in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:startMonitorMetricsCollectionForDMS	Grants the permission to start the collection in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listInstanceStorageForDMS	Grants the permission to query the file system usage of each node in a GaussDB(DWS) cluster in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePerfDashboardForDMS	Grants the permission to delete the monitoring panels of a user in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitorMetricsDetailForDMS	Grants the permission to query metric data in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteSQLProbeForDMS	Grants the permission to delete SQL probes in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:stopAlarmRule	Grants the permission to disable rules on the DMS tenant side.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:stopMonitorMetricsCollectionForDMS	Grants the permission to stop the collection in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listExceptionTableForDMS	Grants the permission to query the skew or dirty page rate of a table in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getInstanceStorageAggForDMS	Grants the permission to query the file system usage of each node in a GaussDB(DWS) cluster in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRSnapShotForDMS	Grants the permission to obtain snapshot records in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPerfMetricsDataForDMS	Grants the permission to obtain all monitoring metrics in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueryForDMS	Grants the permission to obtain all query permissions in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getInstanceIOMetricsForDMS	Grants the permission to query NIC I/O data in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSQLProbeDetailForDMS	Grants the permission to query SQL probe details in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:switchoverMonitorMetricStatusForDMS	Grants the permission to switch the collection switch in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:startAlarmRule	Grants the permission to enable rules on the DMS tenant side.	write	-	-
dws:monitor:getClusterStatus	Grants the permission to query the status of a GaussDB(DWS) cluster in DMS.	read	-	-
dws:cluster:getPerfMetricsDetailForDMS	Grants the permission to obtain monitoring items based on PMID in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSlowInstanceForDMS	Grants the permission to query slow nodes in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDDLExamineConfigForDMS	Grants the permission to query collection configurations in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getMonitoringViewStatusForDMS	Grants the permission to obtain the DMS view status.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:enableAlarm	Grants the permission to enable the alarm function for a cluster on the DMS tenant side.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:createWDRSnapShotForDMS	Grants the permission to add snapshots in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listExecuteStatusForDMS	Grants the permission to query the execution status of a GaussDB(DWS) cluster in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getSlowInstanceDetail-ForDMS	Grants the permission to query slow node details in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:enableSQLProbeForDMS	Grants the permission to update the enabling status of a SQL probe in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRConfigForDMS	Grants the permission to query cluster WDR configurations in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:disableAlarm	Grants the permission to disable the cluster alarm function on the DMS tenant side.	write	-	-
dws:cluster:getMonitoringViewForDMS	Grants the permission to obtain available menus in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getDatabaseUsageForDMS	Grants the permission to query the database usage in a GaussDB(DWS) cluster in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listSQLProbeForDMS	Grants the permission to query SQL probes in pagination mode in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getAlarmMetrics	Grants the permission to query alarm metrics on the DMS tenant side.	read	-	-
dws:monitor:listMetricStatus	Grants the permission to obtain function statuses in DMS.	list	-	-
dws:cluster:listSessionStatusForDMS	Grants the permission to query the session execution status of a GaussDB(DWS) cluster in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadPerfHistoryForDMS	Grants the permission to download historical monitoring trend data in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:addPerfItemForDMS	Grants the permission to add monitoring items in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listClusterSessionForDMS	Grants the permission to obtain all current sessions in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getSQLDiagnosticsForDMS	Grants the permission to query SQL diagnosis details in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateWDRSnapShotForDMS	Grants the permission to update the WDR configurations of a GaussDB(DWS) cluster in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:clearAlarm	Grants the permission to clear alarms on the DMS tenant side.	write	-	-
dws:cluster:executeSQLProbeForDMS	Grants the permission to perform SQL probes in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listQueryStatusForDMS	Grants the permission to obtain the current status of a query in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRReportForDMS	Grants the permission to get report records in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listWLMQueueForDMS	Grants the permission to query the current workload queue in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updatePerfItemForDMS	Grants the permission to update monitoring items in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getQueryCostForDMS	Grants the permission to obtain historical resource consumption in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createWDRReportForDMS	Grants the permission to create WDR reports in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadWDRReportForDMS	Grants the permission to download WDR reports in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDatabaseForDMS	Grants the permission to query all databases in the current cluster in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listUserWLMQueueForDMS	Grants the permission to query the workload queue of a user in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deletePerfItemForDMS	Grants the permission to delete monitoring items in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:monitor:getExceptionAlarmRule	Grants the permission to query exception alarm rules in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getWDRHostForDMS	Grants the permission to query node information in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getHistoryPerfDataForDMS	Grants the permission to query historical monitoring data in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteWDRReportForDMS	Grants the permission to delete WDR reports in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getPerfDetailByDimensionForDMS	Grants the permission to obtain monitored objects based on the cluster ID and dimension in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:downloadPerfHistoryByIdForDMS	Grants the permission to download historical monitoring trend data in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listWaitingWLMForDMS	Grants the permission to obtain queries that are currently waiting in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getQueryPropertyForDMS	Grants the permission to obtain query attributes in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listBucketForDMS	Grants the permission to obtain the OBS bucket list in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getHistoryQueryProperty-tyForDMS	Grants the permission to obtain historical query attributes in DMS.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listExceptionWLMForDMS	Grants the permission to query abnormal tasks in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:terminateQueryForDMS	Grants the permission to terminate queries in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateTaskForDMS	Grants the permission to update tasks in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:retryTaskForDMS	Grants the permission to retry tasks in DMS.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listTaskForDMS	Grants the permission to query tasks in DMS.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getDatabaseOmUserStatus	Grants the permission to obtain the status of an O&M user.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:executeDatabaseOmUserAction	Grants the permission to execute operations of an O&M user.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getClusterInstancesInfo	Grants the permission to query details about the logical cluster of a cluster instance.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:getMetadataSyncStatus	Grants the permission to query the enabling status of DataArts metadata synchronization.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:startMetadataSync	Grants the permission to enable DataArts metadata synchronization.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:stopMetadataSync	Grants the permission to disable DataArts metadata synchronization.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updatePeriodCluster	Grants the permission to update yearly/monthly clusters.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createPeriodCluster	Grants the permission to create yearly/monthly clusters.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteConfigTemplate	Grants the permission to delete configuration templates.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getCountDown	Grants the permission to obtain countdown information.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:getObsHotStorage	Grants the permission to query the OBS data usage of clusters with decoupled storage and compute.	read	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listConfigTemplate	Grants the permission to query configuration parameter templates.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDwsResource	Grants the permission to obtain the cluster instance resource list.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDiscountNode	Grants the permission to query the nodes with discount packages.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:changeToPeriod	Grants the permission to change the billing mode from pay-per-use to yearly/monthly.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:rotateKey	Grants the key rotation permission.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:operateCluster	Allows performing cluster operations, such as restoring and canceling read-only status.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:doUpgrade	Grants the permission to upgrade clusters.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listUpgradePath	Grants the permission to obtain cluster upgrade paths.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dws:cluster:listUpgradeRecord	Grants the permission to obtain cluster upgrade records.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listLogicalClusterPlans	Grants the permission to query scheduled addition and deletion plans.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:createLogicalClusterPlan	Grants the permission to add scheduled addition and deletion plans.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:deleteLogicalClusterPlan	Grants the permission to delete scheduled addition and deletion plans.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:listDatabaseUsers	Grants the permission to query all database users.	list	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:switchLogicalClusterPlan	Grants the permission to enable or disable scheduled addition or deletion plans.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dws:cluster:updateLogicalCluster-Plan	Grants the permission to edit scheduled addition and deletion plans.	write	cluster *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Each API of GaussDB(DWS) usually supports one or more actions. **Table 5-89** lists the supported actions and dependencies.

Table 5-89 Actions and dependencies supported by GaussDB(DWS) APIs

API	Action	Dependency
POST /v2/{project_id}/alarm-subs	dws:alarm:createSubscription	-
DELETE /v2/{project_id}/alarm-subs/{alarm_sub_id}	dws:alarm:deleteSubscription	-
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	-
	dws:cluster:assessRisk	-
POST /v2/{project_id}/clusters/{cluster_id}/eips/{eip_id}	dws:cluster:bindEIP	-
	dws:cluster:bindOrUnbindEIP	
POST /v2/{project_id}/clusters/{cluster_id}/elbs/{elb_id}	dws:cluster:bindELB	-
	dws:cluster:bindOrUnbindELB	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cancel-readonly	dws:cluster:cancelReadonly	-
GET /v2/{project_id}/disaster-recovery/check-name	dws:cluster:checkConnection	-
	dws:cluster:checkDisasterRecoveryName	-

API	Action	Dependency
POST /v1/{project_id}/clusters/{cluster_id}/check-instance-storage	dws:cluster:expandDisk	-
	dws:cluster:resize	-
	dws:cluster:checkRestoreTable	-
	dws:cluster:scaleIn	-
	dws:cluster:checkSupportFine-GrainedBackup	-
	dws:cluster:configureNetwork	-
POST /v1.0/{project_id}/snapshots/{snapshot_id}/linked-copy	dws:cluster:copySnapshot	-
POST /v1.0/{project_id}/clusters	dws:cluster:create	• ecs:cloudServerQuotas:get • ecs:cloudServerFlavors:get • bms:serverQuotas:get • bms:serverFlavors:get • vpc:subnets:get • vpc:vpcs:list • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:securityGroups:get • vpc:securityGroups:create • vpc:securityGroups:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:quotas:list • eip:publicIps:list • eip:publicIps:get • eip:publicIps:create • evs:quotas:get

API	Action	Dependency
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	-
	dws:cluster:createDataSource	-
POST /v2/{project_id}/clusters/{cluster_id}/workload	dws:cluster:setFunctionStatus-ForWLM	-
POST /v1.0/{project_id}/snapshots	dws:cluster:createSnapshot	-
PUT /v2/{project_id}/clusters/{cluster_id}/snapshot-policies	dws:cluster:createSnapshotPolicy	-
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	-

API	Action	Dependency
DELETE /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id}	dws:cluster:deleteDataSource	-
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	-
	dws:cluster:expandWithExistedNodes	-
	dws:cluster:getAntiAffinity	-
	dws:cluster:getCnCount	-
	dws:cluster:listConfig	-
	dws:cluster:getCredential	-
GET /v1.0/{project_id}/clusters/{cluster_id}	dws:cluster:getDetail	-

API	Action	Dependency
GET /v2/{project_id}/disaster-recoveries	dws:cluster:getDisasterRecovery	-
	dws:cluster:getDiskExpandScope	-
	dws:cluster:getEncryptInfo	-
	dws:cluster:getHistoryConfigDetail	-
	dws:cluster:getInstanceDetail	-
GET /v2/{project_id}/disaster-recovery/{disaster_recovery_id}	dws:cluster:getDisasterRecovery	-
	dws:cluster:getInstanceDetail	-
	dws:cluster:getProcessTopo	-
	dws:cluster:getRedistribution	-
	dws::listResourceByTag	-
	dws::countResourceByTag	-
	dws:cluster:getRestoreDatabase	-
	dws:cluster:getRoachConfig	-
	dws:cluster:getSnapshotEncryptInfo	-
	dws:cluster:getSnapshotPolicy	-
	dws:cluster:getSnapshotStorage	-
	dws:cluster:getTaskDetail	-
	dws:cluster:getVolumeInfo	-
GET /v1.0/{project_id}/clusters	dws:cluster:list	-
GET /v1.0/{project_id}/clusters/{cluster_id}/audit-log-records	dws:cluster:listAuditLog	-
	dws:cluster:listBucket	-
GET /v1.0/{project_id}/clusters/{cluster_id}/cns	dws:cluster:listCN	-

API	Action	Dependency
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	-
	dws:cluster:listConnection	-
	dws:cluster:listDatabase	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources	dws:cluster:listDataSource	-
GET /v2/{project_id}/clusters/{cluster_id}/elbs	dws:cluster:listDN	-
	dws:cluster:listELB	-
	dws:cluster:listFlavorForResize	-
	dws:cluster:listFlavorForRestore	-
	dws:cluster:listHistoryConfig	-
	dws:cluster:listNode	-
	dws::listResourceByTag	-
	dws:cluster:listRing	-
GET /v1.0/{project_id}/clusters/{cluster_id}/shrink-numbers	dws:cluster:listRingForScaleIn	-
	dws:cluster:listSchema	-
	dws:cluster:listScaleInNode	-
GET /v1.0/{project_id}/clusters/{cluster_id}/snapshots	dws:cluster:listSnapshot	-
GET /v1.0/{project_id}/snapshots	dws:cluster:listSnapshot	-

API	Action	Dependency
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	-
	dws:cluster:listTable	-
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	-
	dws:cluster:recoverRedistribution	-
POST /v2/{project_id}/clusters/{cluster_id}/redistribution	dws:cluster:redistribution	-
POST /v1.0/{project_id}/clusters/{cluster_id}/reset-password	dws:cluster:resetPassword	-

API	Action	Dependency
POST /v1.0/{project_id}/clusters/{cluster_id}/resize	dws:cluster:resize	-
	dws:cluster:resizeFlavor	-
	dws:cluster:resizeRetry	-
POST /v1.0/{project_id}/clusters/{cluster_id}/restart	dws:cluster:restart	-
POST /v2/{project_id}/disaster-recovery/{disaster_recovery_id}/recovery	dws:cluster:restore	-
	dws:cluster:restoreDisaster	-
POST /v1.0/{project_id}/snapshots/{snapshot_id}/actions	dws:cluster:restoreSnapshot	-
	dws:cluster:restoreTable	-
	dws:cluster:retryELBSwitch	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/maintenance-window	dws:cluster:scaleOut	-
	dws:cluster:setMaintainceWind-ow	-
POST /v1.0/{project_id}/clusters/{cluster_id}/cluster-shrink	dws:cluster:scaleIn	-
POST /v1/{project_id}/snapshots/{snapshot_id}/stop	dws:cluster:stopSnapshot	-
	dws:cluster:suspendRedistribution	-
POST /v1.0/{project_id}/clusters/{cluster_id}/switchover	dws:cluster:switchover	-

API	Action	Dependency
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	-
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	-
PUT /v1.0/{project_id}/clusters/{cluster_id}/ext-data-sources/{ext_data_source_id}	dws:cluster:updateDataSource	-
	dws:cluster:updateInstanceAlias-Name	-
	dws:cluster:updateRoachConfig	-
	dws:cluster:updateScheduleCon-fig	-
	dws:cluster:updateSnapshotPolicy	-
	dws::updateTag	-
POST /v2/{project_id}/event-subs	dws::updateTag	-
	dws:event:createSpec	-
	dws:event:createSubscription	-
DELETE /v2/{project_id}/event-subs/{event_sub_id}	dws:event:deleteSpec	-
	dws:event:deleteSubscription	-
GET /v2/{project_id}/event-subs	dws:event:listSubscription	-
	dws:event:report	-

API	Action	Dependency
PUT /v2/{project_id}/event-subs/{event_sub_id}	dws:event:updateSubscription	-
	dws:service:authorize	-
	dws:service:checkAuthorize	-
	dws:service:getClusterSum	-
	dws:service:getResourceStatistics	-
	dws:service:getStorageStatistics	-
GET /v1.0/{project_id}/dss-pools	dws:service:listDssPools	-
	dws:service:listEps	-
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	-
	dws:cluster:addOperationalTask	-
	dws:cluster:bindManageIp	-
	dws:cluster:checkAccessLts	-
	dws:cluster:checkDisasterRecoveryName	-
	dws:cluster:checkLogicalClusterData	-
	dws:cluster:closeAccessLts	-
	dws:cluster:createDisasterRecovery	-
POST /v2/{project_id}/clusters/{cluster_id}/logical-clusters	dws:cluster:createLogicalCluster	-
	dws:cluster:createApplicationForDM	-
	dws:cluster:createClusterForDM	-
	dws:cluster:createConnectionForDM	-
	dws:cluster:createMappingForDM	-
	dws:cluster:deleteApplicationForDM	-

API	Action	Dependency
	dws:cluster:deleteClusterForDM	-
	dws:cluster:deleteConnection-ForDM	-
	dws:cluster:deleteMappingForDM	-
	dws:cluster:dialsConnection-ForDM	-
	dws:cluster:getApplicationForDM	-
	dws:cluster:listApplicationConfig-ForDM	-
	dws:cluster:listApplicationForDM	-
	dws:cluster:getClusterForDM	-
	dws:cluster:listClusterForDM	-
	dws:cluster:listConfigurationTem-plateForDM	-
	dws:cluster:getConnectionForDM	-
	dws:cluster:listConnectionForDM	-
	dws:cluster:listDependApplica-tionForDM	-
	dws:cluster:getMappingForDM	-
	dws:cluster:listMappingForDM	-
	dws:cluster:listProductForDM	-
	dws:cluster:updateConnection-ForDM	-
	dws:cluster:updateMappingForD M	-
	dws:cluster:startApplication-ForDM	-
	dws:cluster:stopApplication-ForDM	-
	dws:cluster:deleteCrossRegionS-napshotPolicy	-
	dws:cluster:deleteDisasterRecov-ery	-

API	Action	Dependency
DELETE /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}	dws:cluster:deleteLogicalCluster	-
	dws:cluster:deleteOperationalTask	-
	dws:cluster:operateDisasterRecovery	-
PUT /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}	dws:cluster:updateLogicalCluster	-
	dws:cluster:listAllCrossRegionSnapshotConfig	-
	dws:cluster:getDisasterRecoveryProject	-
	dws:cluster:getDisasterRecoveryRegion	-
	dws:cluster:getLastOperationalTask	-
	dws:cluster:getLogicalClusterRings	-
	dws:cluster:getLogicalClusterVolume	-
	dws:cluster:getOperationalTaskConfig	-
	dws:cluster:getOperationalTaskDetail	-
	dws:cluster:getOperationalTaskStatus	-
	dws:cluster:listSnapshotRegion	-
	dws:cluster:getTargetAllCrossRegionSnapshotConfig	-
	dws:cluster:initLogicalClusterSwitch	-
	dws:cluster:listAccessLts	-
	dws:cluster:listDisasterRecovery	-
	dws:cluster:listLogicalCluster	-
	dws:cluster:listLogicalClusterTask	-
	dws:cluster:listOperationalTask	-

API	Action	Dependency
	dws:cluster:openAccessLts	-
	dws:cluster:pauseOperational-Task	-
	dws:cluster:getDisasterRecovery-Detail	-
	dws:cluster:refreshOperational-Task	-
POST /v2/{project_id}/clusters/{cluster_id}/logical-clusters/{logical_cluster_id}/restart	dws:cluster:restartLogicalCluster	-
	dws:cluster:resumeOperational-Task	-
	dws:cluster:setCrossRegionSnap-shotPolicy	-
	dws:cluster:startOperationalTask	-
	dws:cluster:stopOperationalTask	-
	dws:cluster:switchLogicalCluster	-
	dws:cluster:syncCrossRegionBack-upClusterInfo	-
	dws:cluster:syncCrossRegionBack-upConfig	-
	dws:cluster:syncCrossRegionBack-upInfo	-
	dws:cluster:syncLogicalCluster	-
	dws:cluster:updateDisasterReco-veryConfig	-
	dws:cluster:updateOperational-TaskConfig	-
	dws:cluster:updateOperational-Task	-
	dws:cluster:addPlanForWLM	-
	dws:cluster:addPlanStageForWL M	-
	dws:cluster:addQueueForWLM	-
	dws:cluster:addQueueUserForWL M	-
	dws:cluster:deletePlanForWLM	-

API	Action	Dependency
	dws:cluster:deletePlanStage-ForWLM	-
	dws:cluster:deleteQueueForWLM	-
	dws:cluster:deleteQueueUser-ForWLM	-
	dws:cluster:exportPlanForWLM	-
	dws:cluster:getPlanDetailForWLM	-
	dws:cluster:getPlanDetailForWLM	-
	dws:cluster:getPlanLogForWLM	-
	dws:cluster:getPlanQueueForWLM	-
	dws:cluster:getPlanStageForWLM	-
	dws:cluster:listQueueForWLM	-
	dws:cluster:getQueueDetailForWLM	-
	dws:cluster:getQueueRuleForWLM	-
	dws:cluster:importPlanForWLM	-
	dws:cluster:listPlanQueueForWLM	-
	dws:cluster:listPlanForWLM	-
	dws:cluster:listQueueUserForWLM	-
	dws:cluster:listUserForWLM	-
	dws:cluster:getClusterDBInfo-ForWLM	-
	dws:cluster:listClusterPlan-ForWLM	-
	dws:cluster:getClusterSchemaInfoForWLM	-
	dws:cluster:getClusterVersion-ForWLM	-
	dws:cluster:getFunctionStatus-ForWLM	-

API	Action	Dependency
	dws:cluster:setFunctionStatus-ForWLM	-
	dws:cluster:startPlanForWLM	-
	dws:cluster:startPlanForWLM	-
	dws:cluster:stopPlanForWLM	-
	dws:cluster:stopPlanForWLM	-
	dws:cluster:switchPlanStage-ForWLM	-
	dws:cluster:switchPlanStage-ForWLM	-
	dws:cluster:updatePlanStage-ForWLM	-
	dws:cluster:updateQueueBase-ForWLM	-
	dws:cluster:updateQueueResour-ceForWLM	-
	dws:cluster:updateQueueRule-ForWLM	-
	dws:cluster:updateSchemaLimit-ForWLM	-
	dws:cluster:getMonitorConfig-ForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:listClusterInstance-ForDMS	-
	dws:cluster:getDDLExamineDe-tailForDMS	-
	dws:cluster:getClusterDnStream-ForDMS	-
	dws:cluster:listClusterAlarmRule-ForDMS	-
	dws:cluster:getClusterInstance-ForDMS	-
	dws:cluster:getDDLExamineDe-tailForDMS	-
	dws:cluster:getHostNetMetrics-ForDMS	-

API	Action	Dependency
	dws:monitor:getHistoryMetrics	-
	dws:cluster:getMonitoringInfo-ForDMS	-
	dws:cluster:listAlarmRuleForDMS	-
	dws:cluster:updateCollectionI-temForDMS	-
	dws:cluster:doDDLExamineAction ForDMS	-
	dws:cluster:downloadDDLExami-neDetailForDMS	-
	dws:cluster:listInstanceDiskIO-ForDMS	-
	dws:cluster:resetCollectionItem-ForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:listClusterOverview	-
	dws:cluster:getQueryRangeForD MS	-
	dws:monitor:getAlarmConfig	-
	dws:cluster:switchoverCollectionI-temForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:listClusterOverview	-
	dws:monitor:getOSMetrics	-
	dws:cluster:listPerfDashboard-ForDMS	-
	dws:cluster:disableCollectionI-temForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:getAggregationOS-Metrics	-
	dws:cluster:terminateSession-ForDMS	-
	dws:cluster:getPerfDashboardDe-tailForDMS	-

API	Action	Dependency
	dws:monitor:createAlarmRule	-
	dws:cluster:enableCollectionItem-ForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:listInstanceNetwork-MetricsForDMS	-
	dws:cluster:createPerfDashboard-ForDMS	-
	dws:cluster:getMonitorMetrics-ForDMS	-
	dws:monitor:listClusterOverview	-
	dws:cluster:createSQLProbeForDMS	-
	dws:cluster:listInstanceIOStatus-ForDMS	-
	dws:cluster:getMonitorMetricsBy-DimensionForDMS	-
	dws:cluster:updateStorageConfig-ForDMS	-
	dws:monitor:listClusterOverview	-
	dws:monitor:updateAlarmRule	-
	dws:cluster:getInstanceIOAggResultForDMS	-
	dws:cluster:updatePerfDashboard ForDMS	-
	dws:cluster:getMonitorHistory-MetricsCost	-
	dws:monitor:deleteAlarmRule	-
	dws:cluster:updateSQLProbeForDMS	-
	dws:cluster:startMonitorMetrics-CollectionForDMS	-
	dws:cluster:listInstanceStorage-ForDMS	-
	dws:cluster:deletePerfDashboard-ForDMS	-

API	Action	Dependency
	dws:cluster:getMonitorMetrics-DetailForDMS	-
	dws:cluster:deleteSQLProbeForDMS	-
	dws:monitor:stopAlarmRule	-
	dws:cluster:stopMonitorMetrics-CollectionForDMS	-
	dws:cluster:listExceptionTable-ForDMS	-
	dws:cluster:getInstanceStora-geAggForDMS	-
	dws:cluster:getWDRSnapShotForDMS	-
	dws:cluster:getPerfMetricsData-ForDMS	-
	dws:cluster:listQueryForDMS	-
	dws:cluster:getInstanceIOMetrics-ForDMS	-
	dws:cluster:getSQLProbeDetail-ForDMS	-
	dws:cluster:switchoverMonitor-MetricStatusForDMS	-
	dws:monitor:startAlarmRule	-
	dws:monitor:getClusterStatus	-
	dws:cluster:getPerfMetricsDetail-ForDMS	-
	dws:cluster:listSlowInstance-ForDMS	-
	dws:cluster:getDDLExamineCon-figForDMS	-
	dws:cluster:getMonitoringView-StatusForDMS	-
	dws:monitor:enableAlarm	-
	dws:cluster:createWDRSnapShot-ForDMS	-
	dws:cluster:listExecuteStatus-ForDMS	-

API	Action	Dependency
	dws:cluster:listQueryForDMS	-
	dws:cluster:getSlowInstanceDetailForDMS	-
	dws:cluster:enableSQLProbeForDMS	-
	dws:cluster:getWDRConfigForDMS	-
	dws:monitor:disableAlarm	-
	dws:cluster:getMonitoringViewForDMS	-
	dws:cluster:createWDRSnapShotForDMS	-
	dws:cluster:getDatabaseUsageForDMS	-
	dws:cluster:listSQLProbeForDMS	-
	dws:monitor:getAlarmMetrics	-
	dws:monitor:listMetricStatus	-
	dws:cluster:listSessionStatusForDMS	-
	dws:cluster:downloadPerfHistoryForDMS	-
	dws:cluster:addPerfItemForDMS	-
	dws:cluster:listClusterSessionForDMS	-
	dws:cluster:getSQLDiagnosticsForDMS	-
	dws:cluster:updateWDRSnapShot ForDMS	-
	dws:monitor:clearAlarm	-
	dws:cluster:executeSQLProbeForDMS	-
	dws:cluster:listQueryStatusForDMS	-
	dws:cluster:getWDRReportForDMS	-

API	Action	Dependency
	dws:cluster:listWLMQueueForDMS	-
	dws:cluster:updatePerfItemForDMS	-
	dws:cluster:executeSQLProbeForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:cluster:createWDRReportForDMS	-
	dws:cluster:downloadWDRReportForDMS	-
	dws:cluster:listDatabaseForDMS	-
	dws:cluster:listUserWLMQueueForDMS	-
	dws:cluster:deletePerfItemForDMS	-
	dws:cluster:createWDRReportForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:monitor:getExceptionAlarmRule	-
	dws:cluster:getWDRHostForDMS	-
	dws:cluster:getHistoryPerfDataForDMS	-
	dws:cluster:deleteWDRReportForDMS	-
	dws:cluster:getQueryCostForDMS	-
	dws:cluster:getPerfDetailByDimensionForDMS	-
	dws:cluster:downloadPerfHistoryByIdForDMS	-
	dws:cluster:listWaitingWLMForDMS	-
	dws:cluster:downloadWDRReportForDMS	-
	dws:cluster:getQueryPropertyForDMS	-

API	Action	Dependency
	dws:cluster:listBucketForDMS	-
	dws:cluster:getHistoryQueryPropertyForDMS	-
	dws:cluster:listExceptionWLMForDMS	-
	dws:cluster:addPerfItemForDMS	-
	dws:cluster:terminateQueryForDMS	-
	dws:cluster:updateTaskForDMS	-
	dws:cluster:retryTaskForDMS	-
	dws:cluster:listTaskForDMS	-
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	-
GET /v2/{project_id}/clusters/{cluster_id}/instances	dws:cluster:getClusterInstancesInfo	-
	dws:cluster:getMetadataSyncStatus	-
	dws:cluster:startMetadataSync	-
	dws:cluster:stopMetadataSync	-
	dws:cluster:updatePeriodCluster	-
	dws:cluster:createPeriodCluster	-
	dws:cluster:deleteConfigTemplate	-
	dws:cluster:getCountDown	-
	dws:cluster:getObsHotStorage	-
	dws:cluster:listConfigTemplate	-

API	Action	Dependency
	dws:cluster:listDwsResource	-
	dws:cluster:listDiscountNode	-
	dws:cluster:changeToPeriod	-
	dws:cluster:rotateKey	-
	dws:cluster:operateCluster	-
	dws:cluster:setMaintainceWindow	-
	dws:cluster:doUpgrade	-
	dws:cluster:listUpgradePath	-
	dws:cluster:listUpgradeRecord	-
	dws:cluster:delete	-
GET /v1/{project_id}/clusters/{cluster_id}/db-manager/objects	dws:cluster:getDatabaseObjects	-
	dws:cluster:listLogicalClusterPlans	-
	dws:cluster:createLogicalClusterPlan	-
	dws:cluster:deleteLogicalClusterPlan	-
	dws:cluster:listDatabaseUsers	-
	dws:cluster:switchLogicalClusterPlan	-
	dws:cluster:updateLogicalClusterPlan	-
	dws:cluster:getAccessWhitelistStatus	-
POST /v1/{project_id}/clusters/{cluster_id}/access-whitelist	dws:cluster:addAccessWhitelist	-
	dws:cluster:getAccessWhitelist	-

API	Action	Dependency
PUT /v1/{project_id}/clusters/{cluster_id}/access-whitelist/{whitelist_id}	dws:cluster:getAccessWhitelistDetail	-
	dws:cluster:setAccessWhitelistDetail	-
DELETE /v2/{project_id}/clusters/{cluster_id}	dws:cluster:delete	-

Resource Type

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-90**, 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 the SCP statements for GaussDB(DWS).

Table 5-90 Resource types supported by GaussDB(DWS)

Resource Type	URN
cluster	dws:<region>:<account-id>:cluster:<cluster-id>

Conditions

GaussDB(DWS) does not support service-specific condition keys in an SCP.

It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.5.4 MapReduce Service (MRS)

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.

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 MRS, 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 MRS, see **Conditions**.

The following table lists the actions that you can define in SCPs for MRS.

Table 5-91 Actions supported by MRS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
mrs:cluster:createCluster	Grants permission to create a cluster.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
mrs:cluster:deleteCluster	Grants permission to delete a cluster.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:listHosts	Grants permission to query nodes in a cluster.	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:listFiles	Grants permission to query files in a cluster.	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:createJob	Grants permission to execute jobs in a cluster.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:list	Grants permission to query the cluster list.	list	-	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId
mrs:cluster:listJobs	Grants permission to query jobs of a cluster.	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getJob	Grants permission to query job details in a cluster.	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getCluster	Grants permission to query cluster details.	read	mrs:<region>:<account-id>:cluster:<cluster-id>	-
mrs:cluster:resizeNodes	Grants permission to adjust cluster nodes.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:updateClusterName	Grants permission to rename a cluster.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
mrs:cluster:listTags	Grants permission to query cluster tags.	list	-	g:EnterpriseProjectId
mrs:cluster:updateTags	Grants permission to add or delete cluster tags.	tagging	-	g:RequestTag/<tag-key>,g:TagKeys,g:EnterpriseProjectId
mrs:cluster:listClustersByTag	Grants permission to query clusters with specific tags.	list	-	g:RequestTag/<tag-key>,g:TagKeys
mrs:cluster:stopJob	Grants permission to stop cluster jobs.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:deleteJobs	Grants permission to delete cluster jobs in batches.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:stopSql	Grants permission to cancel SQL execution.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:createSql	Grants permission to submit SQL statements for execution.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:listPolicies	Grants permission to obtain all auto scaling policies in a cluster.	list	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
mrs:cluster:updatePolicies	Grants permission to modify the auto scaling policies of a cluster.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getAgencyMapping	Grants permission to obtain user agent information.	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:updateAgencyMapping	Grants permission to update user agent information.	write	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId
mrs:cluster:getSql	Grants permission to obtain the SQL execution result.	read	mrs:<region>:<account-id>:cluster:<cluster-id>	g:EnterpriseProjectId

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-92**, 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 MRS.

Table 5-92 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 SCPs.

It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.5.5 Cloud Search Service (CSS)

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.

Action

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 CSS, see **Resource Type**.
- 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 condition keys defined by CSS, see **Condition**.

The following table lists the actions that you can define in SCP statements for CSS.

Table 5-93 Actions supported by CSS

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:VPCEndpoint:updateWhitelist	Grant the permission to update an existing whitelist of VPC endpoints.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:updateBackupPolicy	Grant the permission to modify or delete log backups.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:setSnapshotPolicy	Grant the permission to set backup policies.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:getSnapshotPolicy	Grant the permission to query backup policies.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:restore	Grant the permission to restore data from a snapshot.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:create	Grant the permission to create a snapshot.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicIPAddress:associates	Grant the permission to enable or disable public access.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicIPAddress:setAccessControl	Grant the permission to manage whitelists for access control.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:get	Grant the permission to query resource tags.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:publicIPAddress:modifyBandwidth	Grant the permission to modify the bandwidth size.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:VPCEndpoint:enableOrDisable	Grant the permission to create or delete a VPCEP.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:getBasicConfigurations	Grant the permission to query basic configurations.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:list	Grant the permission to view the snapshot list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:list	Grant the permission to view logs.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:setSnapshotContigura-tion	Grant the permission to set basic snapshot configurations.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listFlavors	Grant the permission to query the flavor ID list.	list	-	-
css:cluster:listDiskType	Grant the permission to list available disk types.	list	-	-
css:tag:list	Grant the permission to query project tags.	list	cluster *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:VPCEndpoint:manageConnection	Grant the permission to configure the connection of the endpoint.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:listJob	Grant the permission to query the job list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
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 *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:enableAtomaticSnapsot	Grant the permission to set basic configurations for automatic snapshot backup.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:delete	Grant the permission to delete a specified snapshot.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:IKThesaurus:get	Grant the permission to view the custom word dictionary configuration.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:restart	Grant the permission to restart an Elasticsearch cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:cluster:modifySecurityGroup	Grant the permission to modify the cluster security group.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:configurations:list	Grant the permission to query parameter settings.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:delete	Grant the permission to delete a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:modifySpecifications	Grant the permission to modify cluster specifications.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:list	Grant the permission to list cluster information.	list	cluster *	-
css:cluster:scaleOut	Grant the permission to scale out a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:IKThesaurus:load	Grant the permission to load a custom word dictionary.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:configurations:modify	Grant permission to update parameter settings.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:configurations:get	Grant the permission to obtain the parameter list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:IKThesaurus:delete	Grant the permission to delete a word dictionary.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:expand	Grant the permission to scale out the quantity and storage capacity of instances.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:snapshot:disableSnapshotFuction	Grant the permission to disable the cluster snapshot function.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:upgradeCluster	Grant the permission to upgrade clusters or replace nodes.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:VPCEndpoint:listConnection	Grant the permission to query VPCEP connections.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:scaleIn	Grant the permission to scale in a cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:setBasicConfigurations	Grant the permission to set basic configurations.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:addOrDelete	Grant the permission to add or delete resource tags in batches.	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:publicKibana:close	Grant the permission to disable public access.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:edit	Grant the permission to modify cluster tags.	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
css:cluster:create	Grant the permission to create a cluster.	write	cluster *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
css:cluster:toPeriod	Grant the permission to change the billing mode of a cluster to yearly/monthly.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:modifyName	Grant the permission to change the cluster name.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:log:backup	Grant the permission to back up logs.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:closeLogSetting	Grant the permission to disable logging.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:cluster:openLogSetting	Grant the permission to enable logging.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:modifyPassword	Grant the permission to change the cluster password.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicIPAddress:disassociates	Grant the permission to unbind public networks.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:publicKibana:open	Grant the permission to bind public networks.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:tag:delete	Grant the permission to delete a tag.	tagging	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys
css:cluster:shrinkNodes	Grant the permission to scale in a specified node.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:changeMode	Grant the permission to modify the security mode.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:addIndependenceNodes	Grant the permission to add independent master and client nodes.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:cluster:rollingReboot	Grant the permission to perform a rolling restart of an Elasticsearch cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:listActions	Grant the permission to query operation records.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:uploadCerts	Grant the permission to upload certificates.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:deleteCerts	Grant the permission to delete certificates.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listCerts	Grant the permission to query the certificate list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getCertsDetail	Grant the permission to query certificate details.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:deleteConfTemplate	Grant the permission to delete a custom template.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:listConfigTemplate	Grant the permission to query the template list.	list	-	-
css:logstash:confStop	Grant the permission to stop or hot-stop pipeline tasks for data migration.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:logstash:checkConnection	Grant the permission to test the connectivity.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:confDelete	Grant the permission to delete configuration files.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:confStart	Grant the permission to start or hot-start pipeline tasks for data migration.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:getConfDetail	Grant the permission to query the content of configuration files.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:azmigrate	Grant the permission to switch AZs.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:confUpdate	Grant the permission to update configuration files.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:listPipelines	Grant the permission to query the pipeline list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:retryAction	Grant the permission to retry a task or terminate the impact of a task.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:logstash:listConfs	Grant the permission to query the configuration file list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:configFavorites	Grant the permission to add items to a custom template.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listUpgradeCluster	Grant the permission to obtain the upgrade image ID and upgrade details.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:submitConf	Grant the permission to create configuration files.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:list	Grant the permission to query the cluster plug-in list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:getOperationRecords	Grant the permission to query the plug-in operation records.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:delete	Grant the permission to delete plug-ins.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:installOrUninstall	Grant the permission to install or uninstall plug-ins.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:plugin:upload	Grant the permission to upload plug-ins.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:plugin:getDefault	Grant the permission to query default plug-ins.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getAgencies	Grant the permission to obtain agents.	read	-	-
css:cluster:modifyRoute	Grant the permission to modify cluster routes.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getRoutes	Grant the permission to obtain the cluster routes.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:logstash:actionList	Grant the permission to query the cluster task list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
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 *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:queryNeedDeleteInstances	Grant the permission to query the node to be deleted.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:cluster:queryKey	Grant the permission to obtain keys.	read	-	-
css:cluster:queryKeys	Grant the permission to obtain the key list.	list	-	-
css:cluster:getPubliczonePice	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	-	-
css:cluster:checkCssName	Grant the permission to check cluster names.	write	cluster *	-
css:snapshot:deleteAllFailedTask	Grant the permission to delete all failed tasks.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listAiOps	Grant the permission to obtain the detection task list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:deleteAiOps	Grant the permission to delete detection tasks.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listSmnTopics	Grant the permission to obtain the SMN topic list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listElbs	Grant the permission to obtain the list of available load balancers for the current cluster.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:elbSwitch	Grant the permission to enable or disable load balancing.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
css:cluster:createElbListener	Grant the permission to create listeners for the current cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:updateElbListener	Grant the permission to modify listeners for the current cluster.	write	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:getElbDetail	Grant the permission to query information about load balancers used by the current cluster.	read	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
css:cluster:listElbCerts	Grant the permission to obtain the load balancer certificate list.	list	cluster *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Each API of CSS usually supports one or more actions. **Table 5-94** lists the supported actions and dependencies.

Table 5-94 Actions and dependencies supported by CSS APIs

API	Action	Dependency
POST /v1.0/{project_id}/clusters	css:cluster:create	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:securityGroups:list • vpc:securityGroups:get • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get • css:cluster:getAgencies • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass

API	Action	Dependency
POST /v2.0/{project_id}/clusters	css:cluster:create	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:securityGroups:list • vpc:securityGroups:get • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get • css:cluster:getAgencies • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass
POST /v1.0/{project_id}/clusters/{cluster_id}/sg/change	css:cluster:modifySecurityGroup	• vpc:securityGroups:list • vpc:ports:update
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}/changename	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	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
POST /v1.0/{project_id}/clusters/{cluster_id}/role_extend	css:cluster:expand	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
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	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
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	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject

API	Action	Dependency
POST /v1.0/{project_id}/clusters/{cluster_id}/node/offline	css:cluster:shrinkNodes	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
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	• ecs:cloudServerFlavors:get • evs:types:get • vpc:vpcs:list • vpc:subnets:list • vpc:subnets:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:ports:get
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	• iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject
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	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • obs:object:getObject
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	• iam:agencies:pass • obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies
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	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies • iam:agencies:pass
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:enableAtomaticSnapsot	• obs:bucket:createBucket • obs:bucket:headBucket • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:grantRoleToAgency
POST /v1.0/{project_id}/clusters/{cluster_id}/index_snapshot/setting	css:snapshot:setSnapshotContiguration	• obs:bucket:listAllMyBuckets • obs:bucket:getBucketLocation • obs:bucket:getBucketStoragePolicy • iam:agencies:listAgencies • iam:agencies:pass
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:disableSnapshotFuction	-
POST /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/open	css:VPCEndpoint:enableOrDisable	• vpcep:endpoints:create • vpcep:endpoints:list • vpcep:endpoints:get • vpcep:endpoints:delete • vpcep:endpoints:update
PUT /v1.0/{project_id}/clusters/{cluster_id}/vpcepservice/close	css:VPCEndpoint:enableOrDisable	• vpcep::listQuotas • vpcep:endpoints:create • vpcep:endpoints:list • vpcep:endpoints:get • vpcep:endpoints:delete • vpcep:endpoints:update

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/{project_id}/clusters/{cluster_id}/lgsconf/confdetail	css:logstash:getConfDetail	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/update	css:logstash:confUpdate	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listpipelines	css:logstash:listPipelines	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/submit	css:logstash:submitConf	-
POST /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/favorite	css:logstash:configFavorites	-
GET /v1.0/{project_id}/clusters/{cluster_id}/lgsconf/listconfs	css:logstash:listConfs	-
GET /v1.0/{project_id}/lgsconf/template	css:logstash:listConfigTemplate	-
POST /v1.0/{project_id}/clusters/{cluster_id}/certs/upload	css:cluster:uploadCerts	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/certs/{cert_id}/delete	css:cluster:deleteCerts	-

API	Action	Dependency
GET /v1.0/{project_id}/clusters/{cluster_id}/certs	css:cluster:listCerts	-
GET /v1.0/{project_id}/clusters/{cluster_id}/certs/{cert_id}	css:cluster:getCertsDetail	-
POST /v1.0/{project_id}/clusters/{cluster_id}/route	css:cluster:modifyRoute	-
GET /v1.0/{project_id}/clusters/{cluster_id}/route	css:cluster:getRoutes	-
POST /v1.0/{project_id}/clusters/{cluster_id}/ai-ops	css:cluster:createAiOps	-
GET /v1.0/{project_id}/clusters/{cluster_id}/ai-ops	css:cluster:listAiOps	-
DELETE /v1.0/{project_id}/clusters/{cluster_id}/ai-ops/{aiops_id}	css:cluster:deleteAiOps	-
GET /v1.0/{project_id}/domains/{domain_id}/ai-ops/smn-topics	css:cluster:listSmnTopics	• css:cluster:getAgencies • iam:agencies:list • iam:agencies:listAgencies • iam:agencies:listAttachedPolicies • iam:agencies:pass
GET /v1.0/{project_id}/clusters/{cluster_id}/loadbalancers	css:cluster:listElbs	elb:loadbalancers:list

API	Action	Dependency
POST /v1.0/{project_id}/clusters/{cluster_id}/loadbalancers/es-switch	css:cluster:elbSwitch	• elb:loadbalancers:list • iam:agencies:listAgencies • iam:permissions:listRolesForAgency • iam:permissions:listRolesForAgencyOnProject • iam:agencies:pass
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 SCP policy applies to. If you specify a resource type for any action in **Table 5-95**, 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 CSS.

Table 5-95 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 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, css:) apply only to operations of the service. For details, see **Table 5-96**.
  - 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 constitute a complete condition statement. An SCP takes effect only when the statement meets related requirements. 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 SCPs for CSS. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-96 Service-specific condition keys supported by CSS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
css:AssociatePublicIp	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"
      ]
    }
  ]
}
```

5.10.6 Content Delivery & Edge Computing

5.10.6.1 Content Delivery Network (CDN)

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 CDN, 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 CDN, see **Conditions**.

The following table lists the actions that you can define in SCP statements for CDN.

Table 5-97 Actions supported by CDN

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cdn:statistics:queryStats	Querying domain name statistics	list	domain *	g:EnterpriseProjectId
cdn:statistics:downloadExcel	Downloading domain name statistics	list	domain *	g:EnterpriseProjectId
cdn:log:queryLogs	Querying logs	read	domain *	g:EnterpriseProjectId
cdn:charge:modifyChargeMode	Creating or modifying the billing option	write	-	-
cdn:charge:queryChargeMode	Querying the billing option	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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 *	g:EnterpriseProjectId
cdn:configuration:queryDomains	Querying details about a domain name	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyDomainConfigs	Modifying domain name configuration	write	domain *	g:EnterpriseProjectId
cdn:configuration:modifyOriginConfInfo	Modifying the origin server settings	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:log:queryLogs	Querying logs	read	domain *	g:EnterpriseProjectId
cdn:statistics:queryStats	Querying domain name statistics	list	domain *	g:EnterpriseProjectId
cdn:configuration:queryDomainList	Listing domain names	list	domain *	g:EnterpriseProjectId
cdn:configuration:createDomains	Creating a domain name	write	domain *	g:EnterpriseProjectId
cdn:configuration:queryDomains	Querying details about a domain name	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cdn:configuration:deleteDomains	Deleting a domain name	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:disableDomains	Disabling CDN for a domain name	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:enableDomains	Enabling CDN for a domain name	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyOriginServerInfo	Modifying the origin server information	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyOriginConfInfo	Modifying the origin server settings	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryOriginConfInfo	Querying the origin server settings	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyReferConf	Modifying the referer whitelist	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryReferConf	Querying the referer whitelist	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryIpAcl	Querying the IP ACL	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cdn:configuration:modifyIpAcl	Modifying the IP ACL	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryCacheRule	Listing cache rules	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyCacheRule	Modifying a cache rule	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:modifyHttpsConf	Modifying the certificate of a domain name	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryHttpsConf	Querying the HTTPS settings	read	domain	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryIpInfo	Querying the IP address information	list	-	-
cdn:configuration:createResHeader	Creating a response header	write	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:queryResponseHeaderList	Querying response headers	read	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cdn:configuration:batchModifyHttpsConf	Modifying certificates of domain names	write	domain *	g:EnterpriseProjectId
cdn:configuration:queryTags	Listing domain name tags	list	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cdn:configuration:modifyTags	Modifying resource tags	tagging	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
cdn:configuration:deleteTags	Deleting resource tags	tagging	domain *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
cdn:configuration:refreshCache	Purging the cache	write	-	g:EnterpriseProjectId
cdn:configuration:queryRefreshAndPreheatHistoryTask	Querying a cache purge or prefetch task	list	-	-
cdn:configuration:queryCacheHistoryTask	Querying historical cache tasks	list	-	-
cdn:configuration:preheatCache	Modifying cache prefetch settings	write	-	g:EnterpriseProjectId
cdn:configuration:queryQuota	Querying quotas of domain names, cache purge by file, cache purge by directory, and cache prefetch	list	-	-

Each API of CDN usually supports one or more actions. **Table 5-98** lists the supported actions and dependencies.

Table 5-98 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	-
PUT /v1.0/cdn/domains/config-https-info	cdn:configuration:batchModifyHttpsConf	-
GET /v1.0/cdn/domains/https-certificate-info	cdn:configuration:queryDomainList	-

API	Action	Dependencies
PUT /v1.1/cdn/configuration/domains/{domain_name}/configs	cdn:configuration:modifyOriginConfInfo	• cdn:configuration:modifyBusinessType • cdn:configuration:modifyOriginServerInfo • cdn:configuration:modifyBackSourceUrlConfig • cdn:configuration:modifyHttpsConf • cdn:configuration:modifyCacheRule • cdn:configuration:modifyReferConf • cdn:configuration:modifyIpAcl • cdn:configuration:modifyUserAgent • cdn:configuration:modifyUrlAuth • cdn:configuration:createResHeader • cdn:configuration:modifyErrorCodeRedirectRule • cdn:configuration:modifyVideoSeek • cdn:configuration:modifyRemoteAuth • cdn:configuration:modifyServiceArea
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	-
POST /v1.0/cdn/configuration/tags/batch-delete	cdn:configuration:deleteTags	-
POST /v1.0/cdn/content/refresh-tasks	cdn:configuration:refreshCache	-

API	Action	Dependencies
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 SCP policy applies to. If you specify a resource type for any action in **Table 5-99**, 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 CDN.

Table 5-99 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 SCPs. It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.7 Databases

5.10.7.1 Relational Database Service (RDS)

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 RDS, 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 RDS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for RDS.

Table 5-100 Actions supported by RDS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:task:listAll	Grants permission to obtain task information.	list	-	-
rds:tag:list	Grants permission to query project tags.	list	-	-
rds:param:listAll	Grants permission to query parameter templates.	list	-	-
rds:param:listInstanceParamHistories	Grants permission to query change history of instance parameters.	list	-	-
rds:databaseUser:list	Grants permission to query database users.	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:list	Grants permission to query databases.	list	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:backup:list	Grants permission to query backups.	list	-	-
rds:log:setSlowLogSensitiveStatus	Grants permission to show original slow query logs.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:enableSecondLevelMonitoring	Grants permission to enable Monitoring by Seconds.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:instance:tde	Grants permission to enable TDE.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:openReadonly	Grants permission to set an instance to read-only.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifySynchronizeModel	Grants permission to configure the replication mode of a primary/standby instance.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyStrategy	Grants permission to configure the failover priority of a primary/standby instance.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifySSL	Grants permission to enable or disable SSL.	permission_management	-	-
rds:instance:modifyForceSwitch	Grants permission to enable forcible HA switchover.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:setAutoEnlargePolicy	Grants permission to configure a storage autoscaling policy.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyBackupPolicy	Grants permission to configure an automated backup policy.	permission_management	instance	g:EnterpriseProjectId rds:BackupEnabled g:ResourceTag/<tag-key>
rds:instance:extendSpace	Grants permission to scale up storage space of an instance.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:instance:shrinkSpace	Grants permission to scale down storage space of an instance.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:shrink	Grants permission to shrink a database.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:setPolicy	Grants permission to configure a binlog policy.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:auditlog:operate	Grants permission to configure an audit log policy.	permission_management	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getParameter	Grants permission to query the parameter template of an instance.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:param:get	Grants permission to query parameters of a parameter template.	read	-	-
rds:instance:getSecondLevelMonitoringConfig	Grants permission to query the configuration of Monitoring by Seconds.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:log:getErrorLogs	Grants permission to query database error logs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:log:getSlowLogs	Grants permission to query slow query logs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:log:download	Grants permission to download logs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:log:setLogSwitchover	Grants permission to query failover/switchover logs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getAutoEnlargePolicy	Grants permission to query an autoscaling policy.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getBackupPolicy	Grants permission to query a backup policy.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getDBProxy	Grants permission to query information about a database proxy.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getDnsName	Grants permission to query the domain name of an instance.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getMsdtcHosts	Grants permission to query MSDTC hosts.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getProxyFlavors	Grants permission to query available instance classes for a database proxy.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getReplicaStatus	Grants permission to query the replication status of an instance.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:instance:getRestoreTime	Grants permission to query the restoration time range of an instance.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:listAll	Grants permission to query DB instances.	read	-	-
rds:instance:get	Grants permission to query details about an instance.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:getEip	Grants permission to query the EIP bound to an instance.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:update	Grants permission to modify instance information.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateQuota	Grants permission to modify project quotas.	read	-	-
rds:instance:listQuotas	Grants permission to query resource quotas.	read	-	-
rds:instance:deleteTag	Grants permission to delete tags in batches.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
			-	g:RequestTag/<tag-key> g:TagKeys
rds:instance:createTag	Grants permission to add tags in batches.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	g:RequestTag/<tag-key> g:TagKeys
rds:binlog:get	Grants permission to query binlogs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:download	Grants permission to download binlogs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:backup:download	Grants permission to obtain a backup download link.	read	-	-
rds:auditlog:list	Grants permission to query audit logs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:auditlog:download	Grants permission to obtain the link for downloading audit logs.	read	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
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:coldTable:query	Grants permission to query hot and cold data separation.	read	-	-
rds:task:delete	Grants permission to delete tasks from the task center.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:password:update	Grants permission to change a database password.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:param:save	Grants permission to save a parameter template.	write	-	-
rds:param:reset	Grants permission to reset a parameter template.	write	-	-
rds:param:updateTemplate	Grants permission to modify parameters in a parameter template.	write	-	-
rds:instance:updateParameter	Grants permission to modify parameters of an instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:param:delete	Grants permission to delete a parameter template.	write	-	-
rds:param:createTemplate	Grants permission to create a parameter template.	write	-	-
rds:param:copy	Grants permission to replicate a parameter template.	write	-	-
rds:param:apply	Grants permission to apply a parameter template.	write	-	-
rds:instance:tableRestore	Grants permission to restore tables.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:instance:switchover	Grants permission to perform a primary/standby switchover.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:singleToHa	Grants permission to change an instance from single-node to primary/standby.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:haToSingle	Grants permission to change an instance from primary/standby to single-node.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:setRecycleBin	Grants permission to configure a recycling policy.	write	-	-
rds:instance:restoreInPlace	Grants permission to restore data to an existing or original instance.	write	-	-
rds:instance:restart	Grants permission to reboot an instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:stop	Grants permission to stop an instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:start	Grants permission to start an instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifySpec	Grants permission to change instance specifications.	write	-	-
rds:instance:modifySecurityGroup	Grants permission to modify a security group.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:instance:modifyPublicAccess	Grants permission to bind and unbind an EIP.	write	-	-
rds:instance:modifyProxy	Grants permission to enable or disable database proxy.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyPort	Grants permission to change a database port.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyIp	Grants permission to change a floating IP address.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:modifyHost	Grants permission to modify a host.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateDnsName	Grants permission to modify a domain name.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:SetMsdtcHosts	Grants permission to add MSDTC hosts.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateOpsWindow	Grants permission to configure the maintenance window of an instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateName	Grants permission to change an instance name.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:updateRemark	Grants permission to modify an instance description.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:instance:upgradeDatabaseVersion	Grants permission to upgrade the version of an instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:deleteInstance	Grants permission to delete a DB instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:instance:deleteNode	Grants permission to delete a database node.	write	-	-
rds:instance:createDns	Grants permission to create a private DNS server.	write	-	-
rds:instance:create	Grants permission to create a DB instance.	write	-	rds:Encrypted rds:BackupEnabled g:RequestTag/<tag-key> g:TagKeys g:EnterpriseProjectId
rds:instance:batchTableRestore	Grants permission to restore tables to a point in time in batches.	write	-	-
rds:databaseUser:update	Grants permission to modify the remarks of a database account.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:databaseUser:drop	Grants permission to delete a database account.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:databaseUser:create	Grants permission to create a database account.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:databasePrivilege:revoke	Grants permission to revoke permissions of a database account.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:databasePrivilege:grant	Grants permission to authorize a database account.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:drop	Grants permission to delete a database.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:update	Grants permission to modify a database.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:database:createDatabase	Grants permission to create a database.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:merge	Grants permission to merge binlogs.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:binlog:delete	Grants permission to delete binlogs.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:backup:delete	Grants permission to delete a manual backup.	write	-	-
rds:backup:create	Grants permission to create a manual backup.	write	-	-
rds:instance:buildDrRelation	Grants permission to configure DR capabilities for a DR instance.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rds:instance:modifyDRRole	Grants permission to promote a DR instance to primary.	write	instance	g:EnterpriseProjectId g:ResourceTag/<tag-key>
rds:ltsConfig:update	Grants permission to dump logs to LTS.	write	-	-
rds:coldTable:operate	Grants permission to separate hot and cold data.	write	-	-

Each API of RDS usually supports one or more actions. **Table 5-101** lists the supported actions and dependencies.

Table 5-101 Actions and dependencies supported by RDS APIs

API	Action	Dependencies
GET /v3/{project_id}/jobs?id={id}	rds:task:listAll	-
GET /v3/{project_id}/tags	rds:tag:list	-
GET /v3/{project_id}/configurations	rds:param:listAll	-
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}/db_user/detail?page={page}&limit={limit}	rds:databaseUser:list	-
GET /v3/{project_id}/instances/{instance_id}/database/detail?page={page}&limit={limit}	rds:database:list	-
GET /v3/{project_id}/backups?instance_id={instance_id}	rds:backup:list	-
PUT /v3/{project_id}/instances/{instance_id}/slowlog-sensitization/{status}	rds:log:setSlowLogSensitiveStatus	-

API	Action	Dependencies
PUT /v3/{*project_id*}/instances/{*instance_id*}/second-level-monitor	rds:instance:enableSecondLevelMonitoring	-
PUT /v3/{project_id}/instances/{instance_id}/tde	rds:instance:tde	-
PUT /v3/{project_id}/instances/{instance_id}/readonly-status	rds:instance:openReadonly	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/failover/mode	rds:instance:modifySynchronizeModel	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/failover/strategy	rds:instance:modifyStrategy	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/ssl	rds:instance:modifySSL	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:modifyForceSwitch	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/disk-auto-expansion	rds:instance:setAutoEnlargePolicy	-
PUT /v3/{project_id}/instances/{instance_id}/backups/policy	rds:instance:modifyBackupPolicy	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:extendSpace	-
POST /v3/{project_id}/instances/{instance_id}/db_shrink	rds:database:shrink	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/binlog/clear-policy	rds:binlog:setPolicy	-
PUT /v3/{project_id}/instances/{instance_id}/auditlog-policy	rds:auditlog:operate	-
GET /v3/{project_id}/instances/{instance_id}/configurations	rds:instance:getParameter	-
GET /v3/{project_id}/configurations/{config_id}	rds:param:get	-
GET /v3/{*project_id*}/instances/{*instance_id*}/second-level-monitor	rds:instance:getSecondLevelMonitoringConfig	-
POST /v3/{project_id}/instances/{instance_id}/error-logs	rds:log:getErrorLogs	-
POST /v3/{project_id}/instances/{instance_id}/slow-logs	rds:log:getSlowLogs	-

API	Action	Dependencies
POST /v3/{project_id}/instances/{instance_id}/slowlog-download	rds:log:download	-
GET /v3/{*project_id*}/instances/{*instance_id*}/disk-auto-expansion	rds:instance:getAutoEnlargePolicy	-
GET /v3/{project_id}/instances/{instance_id}/backups/policy	rds:instance:getBackupPolicy	-
GET /v3/{*project_id*}/instances/{*instance_id*}/proxy	rds:instance:getDBProxy	-
GET /v3/{project_id}/instances/{instance_id}/dns	rds:instance:getDnsName	-
GET /v3/{project_id}/instances/{instance_id}/msdtc/hosts?offset={offset}&limit={limit}	rds:instance:getMsdtcHosts	-
GET /v3/{project_id}/flavors/{database_name}?version_name={version_name}&spec_code={spec_code}	rds:instance:getProxyFlavors	-
GET /v3/{project_id}/instances/{instance_id}/replication/status	rds:instance:getReplicaStatus	-
GET /v3/{project_id}/instances/{instance_id}/restore-time?date={date}	rds:instance:getRestoreTime	-
GET /v3/{project_id}/instances	rds:instance:listAll	-
GET /v3/{project_id}/instances?id={id}&name={name}&type={type}&datastore_type={datastore_type}&vpc_id={vpc_id}&subnet_id={subnet_id}&offset={offset}&limit={limit}&tags={key}={value}	rds:instance:get	-
GET https://{*Endpoint*}/v3/{project_id}/quotas	rds:instance:listQuotas	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	rds:instance:deleteTag	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	rds:instance:createTag	-
GET /v3/{*project_id*}/instances/{*instance_id*}/binlog/clear-policy	rds:binlog:get	-
GET /v3/{project_id}/backup-files?backup_id={backup_id}	rds:backup:download	-

API	Action	Dependencies
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	-
GET /v3/{*project_id*}/datastores/{*database_name*}	rds:instance:listDatabaseVersion	-
GET /v3/{project_id}/flavors/{database_name}?version_name={version_name}&spec_code={spec_code}	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/{*instance_id*}/password	rds:password:update	-
PUT /v3/{*project_id*}/configurations/{config_id}	rds:param:updateTemplate	-
PUT /v3.1/{project_id}/instances/{instance_id}/configurations	rds:instance:updateParameter	-
DELETE /v3/{project_id}/configurations/{config_id}	rds:param:delete	-
POST /v3/{project_id}/configurations	rds:param:createTemplate	-
POST /v3/{project_id}/configurations/{config_id}/copy	rds:param:copy	-
PUT /v3.1/{*project_id*}/configurations/{config_id}/apply	rds:param:apply	-
POST /v3.1/{project_id}/instances/{instance_id}/restore/tables	rds:instance:tableRestore	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/failover	rds:instance:switchover	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:singleToHa	-
PUT /v3/{project_id}/instances/recycle-policy	rds:instance:setRecycleBin	-

API	Action	Dependencies
POST /v3/{project_id}/instances	rds:instance:restoreInPlace	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:restart	-
POST /v3/{project_id}/instances/{instance_id}/action/shutdown	rds:instance:stop	-
POST /v3/{project_id}/instances/{instance_id}/action/startup	rds:instance:start	-
POST /v3/{*project_id*}/instances/{*instance_id*}/action	rds:instance:modifySpec	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/security-group	rds:instance:modifySecurityGroup	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/public-ip	rds:instance:modifyPublicAccess	-
POST /v3/{*project_id*}/instances/{*instance_id*}/proxy	rds:instance:modifyProxy	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/port	rds:instance:modifyPort	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/ip	rds:instance:modifyIp	-
PUT /v3/{project_id}/instances/{instance_id}/modify-dns	rds:instance:updateDnsName	-
POST /v3/{project_id}/instances/{instance_id}/msdtc/host	rds:instance:SetMsdtcHosts	-
PUT /v3/{*project_id*}/instances/{*instance_id*}/ops-window	rds:instance:updateOpsWindow	-
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}/db-upgrade	rds:instance:upgradeDatabaseVersion	-
DELETE /v3/{project_id}/instances/{instance_id}	rds:instance:deleteInstance	-
POST /v3/{project_id}/instances/{instance_id}/create-dns	rds:instance:createDns	-
POST /v3/{project_id}/instances	rds:instance:create	-

API	Action	Dependencies
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	rds:databaseUser:create	-
DELETE /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:revoke	-
POST /v3/{project_id}/instances/{instance_id}/db_privilege	rds:databasePrivilege:grant	-
DELETE /v3/{project_id}/instances/{instance_id}/database/{db_name}	rds:database:drop	-
POST /v3/{project_id}/instances/{instance_id}/database	rds:database:createDatabase	-
DELETE /v3/{project_id}/backups/{backup_id}	rds:backup:delete	-
POST /v3/{project_id}/backups	rds:backup:create	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:buildDrRelation	-
POST /v3/{project_id}/instances/{instance_id}/action	rds:instance:modifyDRRole	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-102**, 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 RDS.

Table 5-102 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 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, rds:) only apply to operations of the RDS service. For details, see **Table 5-103**.
  - 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.

The following table lists the condition keys that you can define in SCPs for RDS. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-103 Service-specific condition keys supported by RDS

Service-specific Condition Key	Type	Single-valued/ 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.
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.

5.10.7.2 Document Database Service (DDS)

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 DDS, 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 DDS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for DDS.

Table 5-104 Actions supported by DDS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-	-
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	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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 set a policy for audit logs.	permission_management	instance	-
dds:instance:getAuditLogPolicy	Grants permission to query the policy for audit logs.	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	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dds:configuration:delete	Grants permission to delete a parameter template.	write	-	g:EnterpriseProjectId
dds:configuration:update	Grants permission to modify parameters in a parameter template.	write	-	g:EnterpriseProjectId
dds:backup:listAll	Grants permission to query backups.	list	-	-
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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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
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	-	g:EnterpriseProjectId
dds:instance:updateSpec	Grants permission to change DB instance specifications.	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	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dds:instance:switchover	Grants permission to switch over the primary and secondary nodes.	write	instance	-
dds:instance:extendVolume	Grants permission to scale up storage space of a DB instance.	write	instance	-
dds:instance:listAll	Grants permission to query DB instances.	list	-	-
dds:instance:setRecyclePolicy	Grants permission to modify the 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 patch upgrade duration.	read	instance	-
dds:instance:getDiskUsage	Grants permission to query disk usage.	read	instance	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dds:configuration:listAppliedHistory	Grants permission to query application records of a parameter template.	list	-	-
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
dds:task:listAll	Grants permission to query tasks.	list	-	-
dds:task:getDetail	Grants permission to query task details.	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	-
dds:instance:listTags	Grants permission to query tags of a specified DB instance.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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 switch of Show Original Log.	read	instance	-
dds:instance:downloadAuditLog	Grants permission to download audit logs.	read	instance	-
dds:instance:create	Grants permission to create a DB instance.	write	-	dds:Encrypted
				dds:BackupEnabled
dds:instance:restore	Grants permission to restore data to the original instance.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dds:backup:getRestoreTimeList	Grants permission to query the restoration time range.	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	-	-
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	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-
dds:backup:create	Grants permission to create a manual backup for a DB instance.	write	-	-
dds:instance:deleteSession	Grants permission to killing sessions of an instance node.	write	-	-
dds:instance:listSession	Grants permission to query sessions of an instance node.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-
dds:instance:listFlavors	Grants permission to query specifications.	read	-	-
dds:instance:listStorageType	Grants permission to query the database disk type.	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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-
dds:instance:getDetail	Grants permission to query instance details.	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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-	-
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	-	-

Each API of DDS usually supports one or more actions. **Table 5-105** lists the supported actions and dependencies.

Table 5-105 Actions and dependencies supported by DDS APIs

API	Action	Dependencies
POST /v3/{project_id}/instances	dds:instance:create vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-
GET /v3/{project_id}/instances?id={id}&name={name}&mode={mode}&datastore_type={datastore_type}&vpc_id={vpc_id}&subnet_id={subnet_id}&offset={offset}&limit={limit}	dds:instance:listAll	-
DELETE /v3/{project_id}/instances/{instance_id}	dds:instance:delete	-
POST /v3/{project_id}/instances/{instance_id}/restart	dds:instance:restart	-
POST /v3/{project_id}/instances/{instance_id}/enlarge-volume	dds:instance:extendVolume	-
POST /v3/{project_id}/instances/{instance_id}/enlarge	dds:instance:addNode vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get 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	-

API	Action	Dependencies
POST /v3/{project_id}/nodes/{node_id}/unbind-eip	dds:instance:unbindEIP	-
POST /v3/{project_id}/instances/{instance_id}/modify-internal-ip	dds:instance:updateIp	-
POST /v3/{project_id}/instances/{instance_id}/create-ip	dds:instance:createIp	-
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:lisSession	-
POST /v3/{project_id}/nodes/{node_id}/session	dds:instance:deleteSession	-
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?instance_id={instance_id}&backup_id={backup_id}&backup_type={backup_type}&offset={offset}&limit={limit}&begin_time={begin_time}&end_time={end_time}&mode={mode}	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 vpc:vpcs:list vpc:vpcs:get vpc:subnets:get vpc:securityGroups:get vpc:ports:get	-
GET /v3/{projectId}/backups/download-file	dds:backup:download	-

API	Action	Dependencies
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	-
PUT /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	-
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	-

API	Action	Dependencies
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	-
PUT /v3/{project_id}/instances/{instance_id}/reset-password	dds:instance:resetPasswd	-
GET /v3/{project_id}/instances/{instance_id}/db-user/detail? offset ={offset}&limit={limit}&user_name={user_name }&db_name={db_name}	dds:instance:getDatabaseUser	-
GET /v3/{project_id}/instances/{instance_id}/db-roles? role_name={role_name}&db_name={db_name}&offset={offset}&limit={limit}	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 SCP applies to. If you specify a resource type for any action in **Table 5-106**, 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 DDS.

Table 5-106 Resource types supported by DDS

Resource Type	URN	Condition Key
instanceName	dds:<region>:<account-id>:instanceName:<instance-name>	- g:EnterpriseProjectId - g:ResourceTag/<tag-key>

Conditions

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, **DDS:**) only apply to operations of the DDS service. For details, see **Table 5-107**.
  - 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.

The following table lists the condition keys that you can define in SCPs for DDS. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-107 Service-specific condition keys supported by DDS

Service-specific Condition Key	Type	Description
dds:Encrypted	boolean	Filters access by the tag key specifying whether to enable disk encryption transferred in the request parameter.
dds:BackupEnabled	boolean	Filters access by the tag key specifying whether to enable the backup policy transferred in the request parameter.

5.10.7.3 GaussDB

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 GaussDB, 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 GaussDB, see **Conditions**.

The following table lists the actions that you can define in SCP statements for GaussDB.

Table 5-108 Actions supported by GaussDB

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdb:backup:createBackup	Grants permission to create a manual backup for a DB instance.	write	instance	-
gaussdb:backup:deleteBackup	Grants permission to delete a backup.	write	instance	-
gaussdb:backup:listAll	Grants permission to query backups.	list	instance	-
gaussdb:instance:updateBackupPolicy	Grants permission to configure a backup policy.	write	instance	gaussdb:BackupEnabled
gaussdb:param:applyParam	Grants permission to apply a parameter template.	write	instance	-
gaussdb:tag:create	Grants permission to add tags.	tagging	instance	-
gaussdb:instance:bindEIP	Grants permission to bind an EIP.	write	instance	-
gaussdb:instance:check	Grants permission to check instance information.	read	instance	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdb:instance:createInstance	Grants permission to create a DB instance.	write	instance	• gaussdb:BackupEnabled • gaussdb:Encrypted
gaussdb:instance:createDatabase	Grants permission to create a database.	write	instance	-
gaussdb:instance:createDatabaseSchema	Grants permission to create a database schema.	write	instance	-
gaussdb:instance:createDatabaseUser	Grants permission to create a database account.	write	instance	-
gaussdb:instance:deleteInstance	Grants permission to delete a DB instance.	write	instance	-
gaussdb:instance:get	Grants permission to query DB instance information.	read	instance	-
gaussdb:instance:getBackupPolicy	Grants permission to query an automated backup policy.	read	instance	-
gaussdb:instance:getBalanceStatus	Grants permission to check whether host load is unbalanced due to a primary/standby switchover.	read	instance	-
gaussdb:instance:getDiskUsage	Grants permission to query disk usage.	read	instance	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdb:instance:getRecyclePolicy	Grants permission to query the recycling policy.	read	instance	-
gaussdb:instance:downloadSslCert	Grants permission to download the SSL certificate of a DB instance.	read	instance	-
gaussdb:instance:grantDatabasePrivilege	Grants permission to configure permissions of database accounts.	write	instance	-
gaussdb:instance:listAll	Grants permission to query DB instances.	list	instance	-
gaussdb:instance:listPublicIps	Grants permission to query EIPs bound to DB instances.	list	instance	-
gaussdb:instance:listComponents	Grants permission to query instance components.	list	instance	-
gaussdb:instance:listDatabases	Grants permission to query databases.	list	instance	-
gaussdb:instance:listDatabaseUsers	Grants permission to query database users.	list	instance	-
gaussdb:tag:listAll	Grants permission to query resource tags.	list	instance	-
gaussdb:quota:listAll	Grants permission to query quotas.	list	instance	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdb:instance:listRecoverable-Times	Grants permission to query the restoration time range.	list	instance	-
gaussdb:instance:listSchemas	Grants permission to query database schemas.	list	instance	-
gaussdb:instance:renameInstance	Grants permission to change a DB instance name.	write	instance	-
gaussdb:instance:resetPassword	Grants permission to change a database password.	write	instance	-
gaussdb:instance:resizeFlavor	Grants permission to change vCPUs and memory of a DB instance.	write	instance	-
gaussdb:instance:restartInstance	Grants permission to reboot a DB instance.	write	instance	-
gaussdb:instance:setRecyclePolicy	Grants permission to modify the recycling policy.	write	instance	-
gaussdb:instance:switchShard	Grants permission to switch roles of the primary and standby DNs in shards.	write	instance	-
gaussdb:instance:extend	Grants permission to perform scale-out operations.	write	instance	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdb:param:update	Grants permission to modify a parameter template.	write	instance	-
gaussdb:param:check	Grants permission to check a parameter template.	read	instance	-
gaussdb:param:copy	Grants permission to replicate a parameter template.	write	instance	-
gaussdb:param:createParam	Grants permission to create a parameter template.	write	instance	-
gaussdb:param:deleteParam	Grants permission to delete a parameter template.	write	instance	-
gaussdb:param:get	Grants permission to query details about a parameter template.	read	instance	-
gaussdb:param:compare	Grants permission to compare two parameter templates.	read	instance	-
gaussdb:param:listAll	Grants permission to query parameter templates.	list	instance	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdb:param:reset	Grants permission to reset a parameter template.	write	instance	-
gaussdb:quota:update	Grants permission to modify quotas.	write	instance	-
gaussdb:task:listAll	Grants permission to query tasks.	list	instance	-
gaussdb:task:delete	Grants permission to delete a task record.	write	instance	-
gaussdb:task:get	Grants permission to query task details.	read	instance	-

Each API of GaussDB usually supports one or more actions. The following table lists the supported actions and dependencies.

Table 5-109 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
Changing 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 DNs 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 DB instances	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 5-110 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	-
Comparing 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 exists	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 5-111 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 5-112 DB engine versions and specifications

Permission	API	Action	Dependencies
Querying DB engine versions	GET /v3/{project_id}/datastore/versions	gaussdb:instance:listAll	-
Querying instance specifications	GET /v3/{project_id}/flavors?limit={limit}&offset={offset}&ha_mode={ha_mode}&version={version}&spec_code={spec_code}	gaussdb:instance:listAll	-
Querying DB engines	GET /v3/{project_id}/datastores	gaussdb:instance:listAll	-
Querying specifications that a DB instance can be changed to	GET /v3/{project_id}/instances/{instance_id}/available-flavors	gaussdb:instance:listAll	-

Table 5-113 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	-
Configuring permissions of database accounts	POST /v3/{project_id}/instances/{instance_id}/db-privilege	gaussdb:instance:grantDatabasePrivilege	-

Permission	API	Action	Dependencies
Changing 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 users	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 5-114 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 for a DB instance	POST /v3/{project_id}/instances/{instance_id}/tags	gaussdb:tag:create	-

Table 5-115 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 5-116 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 5-117 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 5-118 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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-119**, 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 GaussDB.

Table 5-119 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 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, **gaussdb:**) apply only to operations of the GaussDB service. For details, see **Table 5-120**.

  - 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.

The following table lists the condition keys that you can define in SCPs for GaussDB. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-120 Service-specific condition keys supported by GaussDB

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
gaussdb:BackupEnabled	boolean	Single-valued	Filter access permissions based on the tag key of whether to enable the backup policy transferred in the request parameter. Select **Default** for **Qualifier**.
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 **Default** for **Qualifier**.

5.10.7.4 Data Replication Service (DRS)

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 DRS, 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 DRS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for DRS.

Table 5-121 Actions supported by DRS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:backupMigration-Job:createJob	Grants permission to create a backup migration task.	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:backupMigration-Job:deleteJob	Grants permission to delete a backup migration task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:backupMigration-Job:getJobDetail	Grants permission to query details about a backup migration task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:backupMigration-Job:modifyOfflineTaskInfo	Grants permission to modify information about a backup migration task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getChartMonitor	Grants permission to query report charts.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getDataGuardMonitor	Grants permission to query DR monitoring data.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getLastDataDisplay	Grants permission to query the last DR data.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getRpoAndRto	Grants permission to query the RPO and RTO of a specified task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:compareJob:createDataCompareJob	Grants permission to create a data-level table comparison task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:createObjectCompareJob	Grants permission to create an object-level table comparison task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:deleteDataCompareJob	Grants permission to cancel a data-level table comparison task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getTopicInfo	Grants permission to query information about all created topics.	list	-	-
drs:migrationJob:listAllSmnInfo	Grants permission to query all delivered information.	list	-	-
drs:configuration:getPublicIp	Grants permission to query EIPs or EIP information.	list	-	-
drs:configuration:getVpcs	Grants permission to query VPCs.	list	-	-
drs:configuration:listSubnets	Grants permission to query subnets.	list	-	-
drs:configuration:getFeatures	Grants permission to query the feature whitelist.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:configuration:addTag	Grants permission to add tags.	tagging	-	-
drs:compareJob:exportAccountCompareResult	Grants permission to export and download the comparison result of an account-level comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:exportCompareReport	Grants permission to download the comparison result.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getInstancesTag	Grants permission to batch query tags.	list		
drs:compareJob:exportContentsCompareResult	Grants permission to export the comparison result of a value comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getProjectTags	Grants permission to query project tags.	list	-	-
drs:compareJob:exportLinesCompareResult	Grants permission to export the comparison result of a row comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:compareJob:exportObjectsCompareResult	Grants permission to export the comparison result of an object-level comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getAccountCompare	Grants permission to query the overview of an account-level comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getAccountCompareDetail	Grants permission to query the details of an account-level comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getAccountCompareDetails	Grants permission to query the details of an account-level comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:exportJobs	Grants permission to export data subscription tasks.	list	-	-
drs:compareJob:getAccountDetails	Grants permission to query the overview of a row comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:compareJob:getCompareJobEstimatedTime	Grants permission to query the estimated time of a comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getComparePolicy	Grants permission to query a comparison policy.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:listJobs	Grants permission to query data subscription tasks.	list		
drs:compareJob:getContentCompare	Grants permission to query the overview of a value comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getContentCompareDetail	Grants permission to query the details of a value comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getContentCompareDiff	Grants permission to query the differences of a value comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getDataCompareDetail	Grants permission to query the details of a row comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:compareJob:getDataCompareResult	Grants permission to query the comparison result of a data-level table comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getFlowObjectsCompare	Grants permission to query the overview of a dynamic object-level migration comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getHealthCompareJobDetail	Grants permission to query details of a health comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getLineCompare	Grants permission to query the overview of a row comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getLineCompareDetail	Grants permission to query the details of a row comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getObjectCompare	Grants permission to query the overview of an object-level migration comparison task based on the comparison task ID.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:compareJob:getObjectsCompareDetail	Grants permission to query the details of an object-level comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getObjectsMigrateCompare	Grants permission to query the overview of an object-level migration comparison task based on the task ID.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getObjectsMigrateCompareDetail	Grants permission to query the details of an object-level migration comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getTableCompareDetail	Grants permission to query the details of a data-level table comparison task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:listDataCompare	Grants permission to query data-level table comparison tasks.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:listHealthCompareJobs	Grants permission to query the health comparison report list.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:compareJob:modifyComparePolicy	Grants permission to modify the comparison policy.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:startJob	Grants permission to immediately start a data-level table comparison task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:stopJob	Grants permission to stop a comparison task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:addDataTransformationInfo	Grants permission to add the data processing information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:batchModifyTag	Grants permission to batch add or modify tags.	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:batchReplaceTags	Grants permission to batch reset tags.	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:checkDataTransformationInfo	Grants permission to verify data processing information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:configuration:deleteDataTransformationInfo	Grants permission to delete data processing data.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:deleteSmnInfo	Grants permission to delete a single piece of delivered information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:deleteSmnInfoForTopic	Grants permission to delete a single piece of delivered topic information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:deleteTag	Grants permission to delete a tag.	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:downloadTemplate	Grants permission to download the Excel template before importing object information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getAddColumns	Grant the permission to query data processing information (multiple tables are normalized and multiple columns are added).	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:configuration:getAddColumnsFromDb	Grant the permission to query data processing information (multiple tables are normalized and multiple columns are added) after the task is started.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getFlavorInfo	Grants permission to query the DB engine specifications.	list	-	-
drs:backupMigrationJob:checkOfflineTaskName	Grants permission to verify the name of a backup migration task.	write	-	-
drs:configuration:getColumnInfo	Grants permission to query the column information (column mapping and column filtering) of an object.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getDatabaseName	Grants permission to query the destination database name.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getDatabaseParams	Grants permission to query database parameters.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:backupMigration-Job:exportJobList	Grants permission to export backup migration tasks.	list	-	-
drs:backupMigration-Job:getBackupFileDbList	Grants permission to query databases in a backup file.	list	-	-
drs:configuration:getDataTransformationData	Grants permission to query data processing data.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:backupMigration-Job:getRedisInstList	Grants permission to query Redis DB instances.	list	-	-
drs:backupMigration-Job:listBuckets	Grants permission to query buckets.	list	-	-
drs:backupMigration-Job:listJobs	Grants permission to query backup migration tasks.	list	-	-
drs:backupMigration-Job:listObsObject	Grants permission to query objects in the current bucket.	list	-	-
drs:configuration:getDataTransformationInfo	Grants permission to query data processing information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:listFeature	Grants permission to query supported features.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:configuration:listLinks	Grants permission to query available data flow information.	list	-	-
drs:configuration:getEffectTime	Grants permission to query the database affected time of a specified task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getESConfig	Grants permission to query ElasticSearch configurations.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getInstanceTag	Grants permission to query resource tags.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getSupportDataTransforma-tionType	Grants permission to query data processing data types.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getTableInfo	Grants permission to query the table structure and table data.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:importSmnInfo	Grants permission to enter the notification method and information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:configuration:listTopics	Grants permission to query Kafka topic information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:modifyDatabaseParams	Grants permission to modify database parameters.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:modifyESConfig	Grants permission to modify ElasticSearch configurations.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:modifySmnInfo	Grants permission to modify the notification method and information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:modifyTag	Grants permission to modify resource tags.	tagging	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:configuration:modifyUserInfo	Grants permission to update migration user information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:setMigrationTransSpeed	Grants permission to set the flow control of a migration task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:configuration:getInstanceNum	Grants permission to query the number of tasks.	list	-	-
drs:configuration:getInstanceQuotas	Grants permission to query quotas.	list	-	-
drs:configuration:getQuota	Grants permission to query DRS quotas to a tenant.	list	-	-
drs:migrationJoAb:batchDeleteJobs	Grants permission to batch stop or delete tasks.	write	-	-
drs:configuration:updateDataTransformationInfo	Grants permission to update data processing information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:addSubscribeJob	Grants permission to create a yearly/monthly task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:associateSmnInfo	Grants permission to associate the management-plane topic information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:batchPauseJob	Grants permission to batch suspend tasks.	write	-	-
drs:migrationJob:batchPreCheckJob	Grants permission to batch perform prechecks.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:batchRetryJob	Grants permission to retry a task.	write	-	-
drs:migrationJob:batchSetTransformation	Grants permission to process synchronization objects.	write	-	-
drs:migrationJob:batchStartJob	Grants permission to batch start tasks.	write	-	-
drs:migrationJob:batchTestClusterConnection	Grants permission to test connections in batches (cluster mode).	write	-	-
drs:migrationJob:batchTestConnection	Grants permission to test connections in batches.	write	-	-
drs:migrationJob:downloadBatchCreateTemplate	Grants permission to download the template for creating tasks in batches.	list	-	-
drs:migrationJob:importBatchCreateJobs	Grants permission to import tasks created in batches.	write	-	-
drs:migrationJob:listAsyncJobDetail	Grants permission to query details about the tasks created asynchronously in batches with a specified ID.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:listAsyncJobs	Grants permission to query the list of tasks created asynchronously in batches.	list	-	-
drs:migrationJob:listJobInfo	Grants permission to batch query task details by task ID.	list	-	-
drs:migrationJob:listJobStatus	Grants permission to batch query task status by task ID.	list	-	-
drs:migrationJob:asyncBatchCreateJobByAsyncId	Grants permission to asynchronously create tasks in batches.	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:getJobList	Grants permission to query tasks of a tenant.	list	-	-
drs:migrationJob:listPrecheckResult	Grants permission to query the pre-check results of tasks in batches.	list	-	-
drs:migrationJob:selectDatabaseObject	Grants permission to select the databases or tables to be migrated.	write	-	-
drs:configuration:listEPs	Grants permission to query enterprise projects.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:asyncBatchSaveJob	Grants permission to submit the tasks created asynchronously in batches.	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:asyncBatchUpdateJobByAsyncId	Grants permission to update details about the tasks created asynchronously in batches with a specified ID.	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:migrationJob:batchCreateJob	Grants permission to synchronously create tasks in batches.	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:changeFlavor	Grants permission to change specifications.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getCesJobs	Grants permission to query migration tasks.	list	-	-
drs:migrationJob:changeFlavorByNeed	Grants permission to change node specifications on the pay-per-use page.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:createJob	Grants permission to create a comparison task.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:checkInheritJob	Grants permission to determine whether a task can be inherited.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:checkRestartPoint	Grants permission to check resumable position.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:checkTableExist	Grants permission to query whether the table structure and table data were found.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:copyJobAction	Grants permission to deliver a replication task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:createJob	Grants permission to create an online migration task.	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:createJobs	Grants permission to create a task.	write	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:deleteColumnInfo	Grants permission to delete the column information (column mapping and column filtering) of an object.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:deleteJob	Grants permission to delete online migration task V1.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:downloadDbObjectTemplate	Grants permission to download the object selection template.	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:endJob	Grants permission to stop an online migration task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:exportAddedDeletedObjectsInfo	Grants permission to export added and deleted object information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:compareJob:getCompareResult	Grants permission to query comparison results.	list	-	-
drs:migrationJob:exportErrorInfo	Grants permission to export error information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:exportObjectsSentInfo	Grants permission to export delivered object information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getAccess	Grants permission to query the allowed operations of a specified task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getAggregationTable	Grants permission to query multi-table mapping in the memory.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getCesJob	Grants permission to query migration task details.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjectCollectionStatus	Grants permission to obtain the result of submitting the query of database object information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjects	Grants permission to query database object information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjectsCollectAsync	Grants permission to submit the query of database object information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:getDbObjectTemplateProgress	Grants permission to query the progress of uploading the object import template.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getDbObjectTemplateResult	Grants permission to obtain the result of uploading the object import template.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getFullJobDetails	Grants permission to query details of a full synchronization task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getImportExcelProcess	Grants permission to query the progress of parsing Excel files.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getIncreComponentsDetails	Grants permission to query details about incremental components.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getJob	Grants permission to query details about an online migration task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getJobDetail	Grants permission to query task details.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:getJobMeteringPrice	Grants permission to query task price information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getObjectHasColumn	Grants permission to query objects with column information (column mapping and column filtering).	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getObjectsCompareOverviewa	Grants permission to query data-level streaming comparison.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getObjectSelectInfo	Grants permission to query task object selection information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getOperationInfo	Grants permission to query the operation statistics of a specified task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getProgress	Grants permission to query the migration progress of a specified task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:configuration:listDatabaseParams	Grants permission to query the parameters of the source and destination databases.	list	-	-
drs:migrationJob:getSmnInfo	Grants permission to query a single piece of delivered information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSmnInfoForTopic	Grants permission to query a single piece of delivered topic information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSrcUsers	Grants permission to query the migration users of the source database.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getOpenStreamResult	Grants permission to query the result of enabling the stream mode.	list	-	-
drs:migrationJob:getSupportObject	Grants permission to query whether a task supports object selection and column mapping.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:getSupportSearchObjectType	Grants permission to query the object types that can be queried by a user.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSwitchVipStatus	Grants permission to query dual-VIP switchover result.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:batchDeleteJob	Grants permission to batch delete tasks.	write	-	-
drs:migrationJob:batchOperateJob	Grants permission to batch perform operations on tasks with specified IDs.	write	-	-
drs:migrationJob:getTaskLog	Grants permission to query migration logs.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getTuningParams	Grants permission to query the value of a tuning parameter.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:checkAction	Grants permission to verify a task name.	write	-	-
drs:migrationJob:getUpdateObjectSavingStatus	Grants permission to obtain the progress of saving objects.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:getUserSelectedObjectInfo	Grants permission to query the synchronization mapping selected by a user.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:cloneJobs	Grants permission to clone a MySQL synchronization task.	write	-	-
drs:migrationJob:getUserSetObjectInfo	Grants permission to query synchronized object information.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:jobAction	Grants permission to perform specific operations on a task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:jobUpdateAction	Grants permission to start and stop a task, data capture, and data replay.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:exportJobs	Grants permission to export online migration tasks.	list	-	-
drs:migrationJob:listJobs	Grants permission to query tasks of a tenant.	list	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:getBatchTaskLog	Grants permission to batch query migration logs.	list	-	-
drs:migrationJob:getCountdown	Grants permission to query cloud service countdown information.	list	-	-
drs:migrationJob:getDrsJobByRdsInstanceId	Grants permission to query migration tasks related to RDS DB instances.	list	-	-
drs:migrationJob:listJobs		list	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:migrationJob:listReplayFaultsJobs	Grants permission to query the replay faults.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:modifyColumnInfo	Grants permission to modify the column information (column mapping and column filtering) of an object.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:modifyCommonSetting	Grants permission to update task configurations.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:modifyConflictPolicy	Grants permission to update the conflict policy of a synchronization task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getJobs	Grants permission to query online migration tasks.	list	-	-
drs:migrationJob:getNodeNumByDDMInstance	Grants permission to calculate the number of subtasks based on the number of DDM sharding nodes.	list	-	-
drs:migrationJob:modifyGroupAndStream	Grants permission to enable or disable log reporting to LTS.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getPrecheckResult	Grants permission to query the pre-check result of a migration task.	list	-	-
drs:migrationJob:modifyIncreStartPosition	Grants permission to update the start point of an incremental task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getResourceInstances	Grants permission to query resource instances and associated resources.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:modifyJob	Grants permission to modify an online migration task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:modifySyncTypePolicy	Grants permission to update the synchronization type policy.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:getSubscribeNumber	Grants permission to query the specifications of a yearly/monthly task.	list	-	-
drs:migrationJob:operateJobByJobId	Grants permission to perform operations on a task with a specified ID.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:selectGroupAndStream	Grants permission to query whether the LTS service is enabled for the current task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:sendImportCheck	Grants permission to upload Excel files.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:switchVip	Grants permission to perform dual-VIP switchover.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:updateDDLPolicy	Grants permission to update the DDL filtering policy.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:listProgressInfo	Grants permission to batch query the migration progress and incremental latency by task ID.	list	-	-
drs:migrationJob:updateJobInfo	Grants permission to update details about a task with a specified ID.	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:migrationJob:updateObjectInfo	Grants permission to update database object selection information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:updateTuningParams	Grants permission to modify tuning parameters.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:migrationJob:uploadDbObjectTemplate	Grants permission to upload the object import template.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:downloadReport	Grants permission to download files related to a workload replay task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:replayJob:exportAbnormalSqlData	Grants permission to download abnormal SQL statements during workload replay.	list	job	drs:netType g:EnterpriseProjectId g:RequestTag/<tag-key> g:ResourceTag/<tag-key> g:TagKeys
drs:migrationJob:resourceCheck	Grants permission to check resources for creating an online migration task.	write	-	-
drs:migrationJob:skipPrecheck	Grants permission to skip the pre-check.	write	-	-
drs:replayJob:exportSlowSqlData	Grants permission to export SQL statements during workload replay.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getAbnormalSqlData	Grants permission to query abnormal SQL statements during workload replay.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getAllSqlFile	Grants permission to query full SQL files during workload replay.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getExecuteResultData	Grants permission to query the result of a workload replay task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:replayJob:getExportSlowSqlStatus	Grants permission to query the export status of a workload replay file.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getReplayErrorTemplate	Grants permission to query abnormal SQL templates.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getReplayFile	Grants permission to query files for a workload replay task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:cloudDataGuardJob:getMonitoringData	Grants permission to query DR monitoring data based on the task ID.	list	-	-
drs:cloudDataGuardJob:batchSwitchover	Grants permission to batch perform primary/standby switchover.	write	-	-
drs:cloudDataGuardJob:listJobInfo	Grants permission to query details about DR initialization objects in batches by task ID.	list	-	-
drs:cloudDataGuardJob:listRpoAndRto	Grants permission to batch query RPO and RTO.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:cloudDataGuardJob:listStructProcess	Grants permission to query the progress of DR initialization in batches by task ID.	list	-	-
drs:migrationJob:batchSetSmn	Grants permission to batch set alarm information.	write	-	-
drs:migrationJob:batchSetSpeedLimit	Grants permission to batch set control flow.	write	-	-
drs:migrationJob:batchUpdateDefinerMigrate-Setting	Grants permission to set whether to migrate Definers to the user in batches.	write	-	-
drs:migrationJob:batchUpdateJobInfo	Grants permission to modify task names or descriptions in batches and set exception notification.	write	-	-
drs:migrationJob:batchUpdateUserMigrate	Grants permission to set users and roles to be migrated in batches.	write	-	-
drs:migrationJob:changeSrcOrTargetPwd	Grants permission to change the password of the source or destination database.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:migrationJob:setBatchSyncPolicy	Grants permission to set synchronization policies in batches.	write	-	-
drs:replayJob:getReplayRecord	Grants permission to query reports for a workload replay task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getReplaySlowTemplate	Grants permission to query slow SQL templates.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:getSlowSqlData	Grants permission to query slow SQL statements during workload replay.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:listReplayData	Grants permission to query the statistics list during workload replay.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:createJob	Grants permission to create a data subscription task.	write	job	g:EnterpriseProjectId g:RequestTag/<tag-key> g:TagKeys
drs:subscriptionJob:deleteJob	Grants permission to delete a data subscription task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:subscriptionJob:editJobInfo	Grants permission to edit subscription task information.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:getJobDetail	Grants permission to query details about a data subscription task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:getSubscriptionRecord	Grants permission to query detailed subscription content.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:jobAction	Grants permission to perform operations on a data subscription task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getUserGuideInfo	Grants permission to obtain user guide details.	list	-	-
drs:configuration:modifyUserGuideInfo	Grants permission to update the user guide.	write	-	-
drs:subscriptionJob:updateConsumeTime	Grants permission to modify the consumption time point.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:subscriptionJob:updateJob	Grants permission to modify a data subscription task.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:cloudDataGuardJob:getRdsInstanceCount	Grants permission to query the number of RDS DB instances bound to a specified DDM instance.	list	-	-
drs:configuration:getAvailableNodeType	Grants permission to query available node specifications.	list	-	-
drs:configuration:getAvailableZoneWithoutSell-Out	Grants permission to query available AZs where node specifications are not sold out.	list	-	-
drs:configuration:listAvailableZoneStatus	Grants permission to query the AZ status.	list	-	-
drs:configuration:listAvailableZone	Grants permission to query available AZs.	list	-	-
drs:migrationJob:listAvailableZone	Grants permission to query AZs where specifications are not sold out.	list	-	-
drs:configuration:listResourcesByTag	Grants permission to query tasks by tag.	list	-	-
drs::listDrivers	Grants permission to query drivers.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs::uploadDriver	Grants permission to upload drivers.	write	-	-
drs::deleteDriver	Grants permission to delete drivers.	write	-	-
drs:migrationJob:syncDriver	Grants permission to synchronize drivers.	write	-	-
drs:configuration:modifyConfigInfo	Grants permission to update task parameters.	write	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getJobParameters	Grants permission to query task parameter configuration list.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:configuration:getJobParametersHistory	Grants permission to query the parameter change history of a task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:showReplayTimeScope	Grants permission to query the time window for a workload replay task.	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:showReplayResults	Grants permission to query the result data for a workload replay task.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
drs:replayJob:exportReport	Grants permission to export reports for a workload replay task.	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:showReportExportStatus	Grants permission to query the export status of a workload replay report.	read	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>
drs:replayJob:showReportFileObsUris	Grants permission to query the download address of a workload replay report.	list	job	g:EnterpriseProjectId g:ResourceTag/<tag-key>

Each API of DRS usually supports one or more actions. **Table 5-122** lists the supported actions and dependencies.

Table 5-122 Actions and dependencies supported by DRS APIs

API	Action	Dependencies
DELETE /v3/{project_id}/jobs/batch-jobs	drs:migrationJoAb: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:modifyConfigInfo	-
PUT /v5/{project_id}/jobs/{job_id}/start-position	drs:migrationJob:modifyIncreStartPosition	-
PUT /v5/{project_id}/jobs/{job_id}/update-jdbc-driver	drs:migrationJob:syncDriver	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-123**, 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 DRS.

Table 5-123 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 SCPs. It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.7.5 TaurusDB

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 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 following table lists the actions that you can define in SCP statements for TaurusDB.

Table 5-124 Actions supported by TaurusDB

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:backup:modifyPolicy	Grants permission to configure an automated backup policy.	Permissions management	-	-
gaussdbformysql:param:delete	Grants permission to delete a parameter template.	Permissions management	-	-
gaussdbformysql:instance:switchover	Grants permission to promote a read replica to primary.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:auditlog:list	Grants permission to query audit logs.	List	instance *	g:EnterpriseProjectId
gaussdbformysql:backup:create	Grants permission to create a manual backup.	Write	-	-
gaussdbformysql:backup:delete	Grants permission to delete a backup.	Write	-	-
gaussdbformysql:backup:getRestoreTime	Grants permission to query the restoration time range.	Read	instance *	g:EnterpriseProjectId
gaussdbformysql:backup:list	Grants permission to query backups.	List	-	-
gaussdbformysql:backup:listPolicy	Grants permission to query backup policies.	List	instance *	g:EnterpriseProjectId
gaussdbformysql:database:create	Grants permission to create a database.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:database:delete	Grants permission to delete a database.	Write	instance *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:database:list	Grants permission to query databases.	List	instance *	g:EnterpriseProjectId
gaussdbformysql:database:modify	Grants permission to modify database information.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:getSecondLevelMonitoring-Config	Grants permission to query the configuration of Monitoring by Seconds.	Read	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:addReadOnlyNodes	Grants permission to add read replicas.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:create	Grants permission to create a DB instance.	Write	-	g:EnterpriseProjectId
gaussdbformysql:instance:delete	Grants permission to delete a DB instance.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:deleteSqlFilterRules	Grants permission to delete concurrency control rules of SQL statements.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:get	Grants permission to obtain the details about a DB instance.	Read	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:getDcc	Grants permission to query the details about a dedicated resource pool.	Read	-	-
gaussdbformysql:instance:getSqlFilterRule	Grants permission to query concurrency control rules of SQL statements.	Read	instance *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:instance:getSqlFilterStatus	Grants permission to query whether SQL Statement Concurrency Control is enabled.	Read	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:list	Grants permission to query DB instances.	List	-	-
gaussdbformysql:proxy:list	Grants permission to query proxy instances.	List	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:listSpec	Grants permission to query proxy instance specifications.	List	-	-
gaussdbformysql:instance:listDcc	Grants permission to query dedicated resources.	List	-	-
gaussdbformysql:instance:listEngine	Grants permission to query the DB engine information.	List	-	-
gaussdbformysql:instance:listSpec	Grants permission to query specifications.	List	-	-
gaussdbformysql:auditlog:operate	Grants permission to enable or disable SQL Explorer.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:bindPublicIp	Grants permission to bind an EIP.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:deleteReadOnlyNodes	Grants permission to delete a read replica.	Write	instance *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:instance:modifyVip	Grants permission to change private IP address.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyMaintenanceWindow	Grants permission to change a maintenance window of a DB instance.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifySecondLevelMonitor-Policy	Grants permission to change the collection period of Monitoring by Seconds.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyPassword	Grants permission to change the password of a DB instance.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyPort	Grants permission to change a DB instance port.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifySecurityGroup	Grants permission to change a security group.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifySSL	Grants permission to enable or disable SSL.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifyStorageSize	Grants permission to scale down storage of a DB instance.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:rename	Grants permission to change a DB instance name.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:unbindPublicIp	Grants permission to unbind an EIP.	Write	instance *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:instance:upgrade	Grants permission to upgrade the kernel version of a DB instance.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:user:create	Grants permission to create a database account.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:addNodes	Grants permission to add proxy nodes.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:create	Grants permission to create a proxy instance.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:delete	Grants permission to delete a proxy instance.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:modifySpec	Grants permission to change specifications of a proxy instance.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:modifyWeight	Grants permission to change read weights of nodes for a proxy instance.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:modifySpec	Grants permission to change instance specifications.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:restart	Grants permission to reboot a DB instance.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:restoreInPlace	Grants permission to restore data to an existing instance.	Permissions management	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:instance:setSqlFilterRules	Grants permission to configure concurrency control rules of SQL statements.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:setSqlFilterStatus	Grants permission to enable or disable SQL statement concurrency control.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:instance:tableRestore	Grants permission to restore tables to a point in time.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:tag:deal	Grants permission to add or delete resource tags.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:log:getErrorLogs	Grants permission to query error logs.	Read	instance *	g:EnterpriseProjectId
gaussdbformysql:log:getSlowLogs	Grants permission to query slow query logs.	Read	instance *	g:EnterpriseProjectId
gaussdbformysql:param:apply	Grants permission to apply a parameter template.	Permissions management	-	-
gaussdbformysql:param:create	Grants permission to create a parameter template.	Write	-	-
gaussdbformysql:param:get	Grants permission to obtain details about a parameter template.	Read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:param:list	Grants permission to query parameter templates.	List	-	-
gaussdbformysql:param:update	Grants permission to modify parameters in a parameter template.	Write	-	-
gaussdbformysql:proxy:modifyConsistency	Grants permission to change session consistency of a proxy instance.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:modifyTransactionSplit	Grants permission to enable or disable transaction splitting of a proxy instance.	Permissions management	instance *	g:EnterpriseProjectId
gaussdbformysql:quota:list	Grants permission to query quotas.	Read	-	-
gaussdbformysql:quota:modify	Grants permission to modify quotas.	Write	-	-
gaussdbformysql:tag:list	Grants permission to query tags.	List	-	-
gaussdbformysql:task:delete	Grants permission to delete a task record.	Write	-	-
gaussdbformysql:task:list	Grants permission to obtain tasks.	List	-	-
gaussdbformysql:user:delete	Grants permission to delete a database user.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:user:grantPrivilege	Grants permission to change permissions of a database user.	Write	instance *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
gaussdbformysql:user:list	Grants permission to query database users.	List	instance *	g:EnterpriseProjectId
gaussdbformysql:user:modify	Grants permission to query remarks of a database user.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:user:revokePrivilege	Grants permission to delete permissions of a database user.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:user:updatePassWord	Grants permission to change password of a database user.	Write	instance *	g:EnterpriseProjectId
gaussdbformysql:proxy:switchConnectionPoolType	Grants permission to change the connection pool type of a proxy instance.	Permissions management	instance *	g:EnterpriseProjectId

Each API of TaurusDB usually supports one or more actions. **Table 5-125** lists the supported actions and dependencies.

Table 5-125 Actions and dependencies supported by TaurusDB APIs

API	Action	Dependencies
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	-

API	Action	Dependencies
GET /v3.1/{project_id}/instances	gaussdbformysql:instance:list	-
POST /v3/{project_id}/instances/{instance_id}/restart	gaussdbformysql:instance:restart	-
DELETE /v3/{project_id}/instances/{instance_id}	gaussdbformysql:instance:delete	-
GET /v3.1/{project_id}/instances/{instance_id}	gaussdbformysql:instance:get	-
GET /v3.1/{project_id}/instances/details	gaussdbformysql:instance:get	-
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	-
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	-

API	Action	Dependencies
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	-

API	Action	Dependencies
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	-
POST /v3/{project_id}/quotas	gaussdbformysql:quota:modify	-
PUT /v3/{project_id}/quotas	gaussdbformysql:quota:modify	-
POST /v3/{project_id}/backups/create	gaussdbformysql:backup:create	-
GET /v3/{project_id}/backups	gaussdbformysql:backup:list	-

API	Action	Dependencies
GET /v3/{project_id}/instances/{instance_id}/backups/policy	gaussdbformysql:backup:listPolicy	-
GET /v3/{project_id}/configurations	gaussdbformysql:param:list	-
POST /v3/{project_id}/configurations	gaussdbformysql:param:create	-
DELETE /v3/{project_id}/configurations/{configuration_id}	gaussdbformysql:param:delete	-
GET /v3/{project_id}/configurations/{configuration_id}	gaussdbformysql:param:get	-
PUT /v3/{project_id}/configurations/{configuration_id}	gaussdbformysql:param:update	-
PUT /v3/{project_id}/configurations/{configuration_id}/apply	gaussdbformysql:param:apply	-
GET /v3/{project_id}/instances/{instance_id}/tags	gaussdbformysql:tag:list	-
GET /v3/{project_id}/tags	gaussdbformysql:tag:list	-
POST /v3/{project_id}/instances/{instance_id}/tags/action	gaussdbformysql:tag:deal	-

API	Action	Dependencies
PUT /v3/{project_id}/instances/{instance_id}/monitor-policy	gaussdbformysql:instance:modifySecondLevelMonitorPolicy	-
GET /v3/{project_id}/instances/{instance_id}/monitor-policy	gaussdbformysql:instance:getSecondLevelMonitoringConfig	-
POST /v3/{project_id}/instances/{instance_id}/nodes/{node_id}/restart	gaussdbformysql:instance:restart	-
POST /v3/{project_id}/instance/{instance_id}/audit-log/switch	gaussdbformysql:auditlog:operate	-
GET /v3/{project_id}/instance/{instance_id}/audit-log/switch-status	gaussdbformysql:auditlog:list	-
GET /v3/{project_id}/jobs	gaussdbformysql:task:list	-
POST /v3/{project_id}/instances/{instance_id}/db-users	gaussdbformysql:user:create	-
GET /v3/{project_id}/instances/{instance_id}/db-users	gaussdbformysql:user:list	-
DELETE /v3/{project_id}/instances/{instance_id}/db-users	gaussdbformysql:user:delete	-

API	Action	Dependencies
PUT /v3/{project_id}/instances/{instance_id}/db-users/comment	gaussdbformysql:user:modify	-
PUT /v3/{project_id}/instances/{instance_id}/db-users/password	gaussdbformysql:user:updatePassWord	-
POST /v3/{project_id}/instances/{instance_id}/db-users/privilege	gaussdbformysql:user:grantPrivilege	-
DELETE /v3/{project_id}/instances/{instance_id}/db-users/privilege	gaussdbformysql:user:revokePrivilege	-
GET /v3/{project_id}/instances/{instance_id}/databases/charsets	gaussdbformysql:database:list	-
POST /v3/{project_id}/instances/{instance_id}/databases	gaussdbformysql:database:create	-
GET /v3/{project_id}/instances/{instance_id}/databases	gaussdbformysql:database:list	-
DELETE /v3/{project_id}/instances/{instance_id}/databases	gaussdbformysql:database:delete	-
PUT /v3/{project_id}/instances/{instance_id}/databases/comment	gaussdbformysql:database:modify	-

API	Action	Dependencies
POST /v3/{project_id}/instances/{instance_id}/sql-filter/switch	gaussdbformysql:instance:setSqlFilterStatus	-
GET /v3/{project_id}/instances/{instance_id}/sql-filter/switch	gaussdbformysql:instance:getSqlFilterStatus	-
PUT /v3/{project_id}/instances/{instance_id}/sql-filter/rules	gaussdbformysql:instance:setSqlFilterRules	-
GET /v3/{project_id}/instances/{instance_id}/sql-filter/rules	gaussdbformysql:instance:getSqlFilterRule	-
DELETE /v3/{project_id}/instances/{instance_id}/sql-filter/rules	gaussdbformysql:instance:deleteSqlFilterRules	-
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	-

API	Action	Dependencies
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	-

API	Action	Dependencies
PUT /v3/{project_id}/instances/{instance_id}/alias	gaussdbformysql:instance:rename	-
DELETE /v3/{project_id}/backups/{backup_id}	gaussdbformysql:backup:delete	-
POST /v3.1/{project_id}/instances/{instance_id}/restore/tables	gaussdbformysql:instance:tableRestore	-
POST /v3/{project_id}/instances/restore	gaussdbformysql:instance:restoreInPlace	-
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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-126**, 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 type that you can define in identity policy statements for TaurusDB.

Table 5-126 Resource type supported by TaurusDB

Resource Type	URN
Instance	gaussdbformysql:<region>:<account-id>:instance:<instance-id>

Conditions

TaurusDB 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.

5.10.8 Security & Compliance

5.10.8.1 Advanced Anti-DDoS (AAD)

5.10.8.1.1 Cloud Native Anti-DDoS Basic (Anti-DDoS)

The Service Control Policies (SCPs) in the Organizations service can use these authorization elements to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permission 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 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 SCP 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 resource types defined by Anti-DDoS, see **Resources**.

- The **Condition Key** column includes keys that you can specify in the Condition element of a SCP 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 condition keys defined by Anti-DDoS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Anti-DDoS.

Table 5-127 Actions supported by Anti-DDoS

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
anti-ddos:task:list	Grant permission to query Anti-DDoS tasks.	list	-	-
anti-ddos:quota:list	Grant permission to query quotas.	list	-	-
anti-ddos:optionalDefensePolicy:list	Grant permission to query Anti-DDoS protection specifications.	list	-	-
anti-ddos:logConfig:update	Grant permission to update LTS configurations.	write	-	-
anti-ddos:logConfig:get	Grant permission to query LTS configurations.	read	-	-
anti-ddos:ip:updateDefensePolicy	Grant permission to update Anti-DDoS.	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:untagResource	Grant permission to delete tags in batches.	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
anti-ddos:ip:tagResource	Grant permission to add tags in batches.	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:listTagsForResource	Grant permission to query resource tags.	list	ip *	-
anti-ddos:ip:listDefenseStatuses	Grant permission to query EIP protection statuses.	list	ip *	-
anti-ddos:ip:getWeeklyReport	Grant permission to query weekly protection statistics.	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:getDefenseStatus	Grant permission to query the protection status of an EIP.	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:getDefensePolicy	Grant permission to query Anti-DDoS.	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:getDailyTrafficReport	Grant permission to query protected traffic of an EIP.	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:getDailyEventReport	Grant permission to query abnormal events of an EIP.	read	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
anti-ddos:ip:enableDefensePolicy	Grant permission to enable Anti-DDoS.	write	ip *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
anti-ddos:defaultDefensePolicy:get	Grant permission to query default Anti-DDoS protection policies.	read	-	-
anti-ddos:defaultDefensePolicy:delete	Grant permission to delete default Anti-DDoS protection policies.	write	-	-
anti-ddos:defaultDefensePolicy:create	Grant permission to configure default Anti-DDoS protection policies.	write	-	-
anti-ddos:alertConfig:update	Grant permission to update alarm configurations.	write	-	-
anti-ddos:alertConfig:get	Grant permission to query alarm configurations.	read	-	-

An Anti-DDoS API usually corresponds to one or more actions. **Table 5-128** lists the supported actions and dependencies.

Table 5-128 Actions and dependencies supported by Anti-DDoS APIs

API	Action	Dependency
GET /v1/{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:optionalDefense-Policy:list	-

API	Action	Dependency
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	Dependency
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	-
GET /v1/{project_id}/antiddos/immediate_protection	anti-ddos:ip:enableDefensePolicy	-

API	Action	Dependency
DELETE /v1/{project_id}/antiddos/{floating_ip_id}	anti-ddos:ip:disableDefensePolicy	-
GET /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	-
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 SCP policy applies to. If you specify a resource type for any action in **Table 5-129**, the resource URN must be specified in the SCP 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 SCP policy statements for Anti-DDoS.

Table 5-129 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 SCP policies.

Anti-DDoS can use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.8.1.2 Cloud Native Anti-DDoS Advanced (CNAD)

The Service Control Policies (SCPs) in the Organizations service can use these authorization elements to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permission 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 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 SCP 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 CNAD, see **Resource**.
- The **Condition Key** column includes keys that you can specify in the Condition element of a SCP 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 CNAD, see **Conditions**.

The following table lists the actions that you can define in SCP statements for CNAD.

Table 5-130 Actions supported by CNAD

Action	Description	Access Level	Resource Type (* required)	Condition Key
cnad:schedule:update	Grant permission to update scheduling specifications.	write	schedule *	-
cnad:schedule:list	Grant permission to query the scheduling rule list.	list	schedule *	-
cnad:schedule:get	Grant permission to query scheduling rules.	read	schedule *	-
cnad:schedule:delete	Grant permission to delete scheduling rules.	write	schedule *	-
cnad:schedule:create	Grant permission to create scheduling rules.	write	schedule *	-
cnad:quota:update	Grant permission to modify quotas.	write	-	-
cnad:blockade:release	Grant permission to unblock IP addresses.	write	-	-
cnad:blockade:list	Grant permission to query the blocking list.	list	-	-
cnad:blockade:get	Grant permission to query blocking records.	read	-	-
cnad:alarmConfig:update	Grant permission to modify alarm notifications.	write	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
cnad:alarmConfig:create	Grant permission to create alarm notifications.	write	-	-
cnad:alarmConfig:delete	Grant permission to delete alarm notifications.	write	-	-
cnad:alarmConfig:get	Grant permission to query alarm notifications.	read	-	-
cnad:attackReport:list	Grant permission to query attack events.	list	-	-
cnad:attackReport:update	Grant permission to update attack event configurations.	write	-	-
cnad:attackTop:list	Grant permission to query top 10 attacked IP addresses.	list	-	-
cnad:attackTypeReport:list	Grant permission to query attack type distribution.	list	-	-
cnad:bindPolicy:create	Grant permission to bind protection policies to protected IP addresses.	write	-	-
cnad:blackWhiteIpList:create	Grant permission to create an IP address blacklist or whitelist.	write	-	-
cnad:blackWhiteIpList:delete	Grant permission to delete an IP address blacklist or whitelist.	write	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
cnad:cleanCountReport:list	Grant permission to query the DDoS protection trend.	list	-	-
cnad:cleanKbpsReport:list	Grant permission to query statistics on peak scrubbing traffic.	list	-	-
cnad:cleanScaleDropList:list	Grant permission to query the scrubbing scope.	list	-	-
cnad:countReport:get	Grant permission to query statistics.	read	-	-
cnad:ipTag:put	Grant permission to update the tags of protected IP addresses.	write	-	-
cnad:package:create	Create an instance.	write	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cnad:package:get	Grant permission to query an instance.	read	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cnad:package:list	Query the DB instance list.	list	package *	-
cnad:package:put	Grant permission to update an instance.	write	package *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
cnad:packageDropList:list	Grant permission to query the instance summary list.	list	-	-
cnad:packetAttackReport:list	Grant permission to query attack data packets.	list	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
cnad:policy:create	Grant permission to create protection policies.	write	policy *	g:EnterpriseProjectId
cnad:policy:delete	Grant permission to delete protection policies.	write	policy *	g:EnterpriseProjectId
cnad:policy:get	Grant permission to query details about a protection policy.	read	policy *	g:EnterpriseProjectId
cnad:policy:list	Grant permission to query protection policy details.	list	policy *	-
cnad:policy:put	Grant permission to update protection policies.	write	policy *	g:EnterpriseProjectId
cnad:policyDropList:list	Grant permission to query the protection policy list.	list	-	-
cnad:protectedIp:create	Grant permission to bind protected IP addresses to an instance.	write	-	-
cnad:protectedIp:list	Grant permission to query the protected IP address list.	list	-	-
cnad:protectedIpDropList:list	Grant the permission to query the protected IP address drop-down list.	list	-	-
cnad:quota:get	Grant permission to query quotas.	read	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
cnad:securityStatusReport:get	Grant permission to query asset security status.	read	-	-
cnad:trafficAttackReport:list	Grant permission to query attack traffic.	list	-	-
cnad:policy:unbind	Grant permission to remove a protection policy from a protected IP address.	write	-	-
cnad:weekStatisticsReport:get	Grant permission to query weekly security statistics.	read	-	-

Each API of CNAD usually supports one or more actions. **Table 5-131** lists the supported actions and dependencies.

Table 5-131 Actions and dependencies supported by CNAD APIs

API	Action	Dependency
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	-

API	Action	Dependency
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:blackWhiteIpList:create	-
POST /v1/cnad/policies/{policy_id}/ip-list/delete	cnad:blackWhiteIpList: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	-
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	-

API	Action	Dependency
GET /v1/cnad/packages/{package_id}/unbound-protected-ips	cnad:protectedIpDrop-List:list	-
POST /v1/cnad/policies/{policy_id}/unbind	cnad:policy:unbind	-

Resource

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-132**, the resource URN must be specified in the SCP 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 SCP policy statements for CNAD.

Table 5-132 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 SCP policies.

CNAD can use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.8.1.3 Advanced Anti-DDoS (AAD)

The Service Control Policies (SCPs) in the Organizations service can use these authorization elements to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permission 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 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 SCP 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 AAD, see **Resources**.
- The **Condition Key** column includes keys that you can specify in the Condition element of a SCP 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 AAD, see **Conditions**.

The following table lists the actions that you can define in SCP statements for AAD.

Table 5-133 Actions supported by AAD

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aad:alarmConfig:create	Create alarm settings.	write	alarmConfig *	-
aad:alarmConfig:put	Modify alarm settings.	write	alarmConfig *	-
aad:alarmConfig:get	Query alarm settings.	read	alarmConfig *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aad:alarmConfig:delete	Delete alarm settings.	write	alarmConfig *	-
aad:certificate:delete	Delete certificates.	write	certificate *	-
aad:certificate:list	Query certificates.	list	certificate *	-
aad:certificate:set	Modify domain name certificates.	write	certificate *	-
			domain *	g:EnterpriseProjectId
aad:dashboard:delete	Delete report log configurations.	write	-	-
aad:dashboard:get	Obtain report data and log configurations.	read	-	-
aad:dashboard:set	Modify report log configurations.	write	-	-
aad:domain:create	Add protected domain names.	write	domain *	g:EnterpriseProjectId
aad:domain:delete	Delete protected domain names.	write	domain *	g:EnterpriseProjectId
aad:domain:get	Query domain name details.	read	domain *	g:EnterpriseProjectId
aad:domain:list	Query the domain name list.	list	domain *	g:EnterpriseProjectId
aad:domain:put	Modify domain protection attributes.	write	domain *	g:EnterpriseProjectId
aad:forwardingRule:create	Add forwarding rules.	write	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:delete	Delete forwarding rules.	write	forwardingRule *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aad:forwardingRule:get	Query forwarding rules.	read	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:list	Export forwarding rules.	list	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:put	Modify the back-to-source IP address permissions in the forwarding rule.	write	forwardingRule *	g:EnterpriseProjectId
aad:instance:create	Create an instance.	write	instance *	g:EnterpriseProjectId
aad:instance:get	Query instance attributes.	read	instance *	g:EnterpriseProjectId
aad:instance:list	Query the DB instance list.	list	instance *	g:EnterpriseProjectId
aad:instance:put	Modify instance attributes.	write	instance *	g:EnterpriseProjectId
aad:policy:create	Add protection rules.	write	policy *	g:EnterpriseProjectId
aad:policy:delete	Delete protection rules.	write	policy *	g:EnterpriseProjectId
aad:policy:get	Query protection rule details.	read	policy *	g:EnterpriseProjectId
aad:policy:list	Query protection rules.	list	policy *	g:EnterpriseProjectId
aad:policy:put	Modify protection rules.	write	policy *	g:EnterpriseProjectId
aad:quotas:get	Query protection specifications.	read	-	-
aad:whiteBlackIpRule:create	Add IP addresses to the blacklist or whitelist.	write	whiteBlackIpRule *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aad:whiteBlackIpRule:delete	Delete IP addresses from the blacklist or whitelist.	write	whiteBlackIpRule *	g:EnterpriseProjectId
aad:whiteBlackIpRule:list	Query the protection blacklist and whitelist.	list	whiteBlackIpRule *	g:EnterpriseProjectId
aad:protectedIp:put	Modify the labels of protected objects.	write	-	-
aad:protectedIp:list	Query the protected object list.	list	-	-
aad:package:put	Modify the protection package.	write	package *	-
aad:package:list	Query the protected IP address list.	list	package *	-
aad:block:put	Unblock IP addresses.	write	-	-
aad:block:list	Query the blocked IP address list.	list	-	-
aad:block:get	Query blocking and unblocking information.	read	-	-
aad:alarmConfig:create	Create alarm settings.	write	alarmConfig *	-
aad:alarmConfig:put	Modify alarm settings.	write	alarmConfig *	-
aad:alarmConfig:get	Query alarm settings.	read	alarmConfig *	-
aad:alarmConfig:delete	Delete alarm settings.	write	alarmConfig *	-
aad:certificate:delete	Delete a certificate.	write	certificate *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aad:certificate:list	Query certificates.	list	certificate *	-
aad:certificate:set	Modify the certificate for a domain name.	write	certificate *	-
			domain *	g:EnterpriseProjectId
aad:dashboard:delete	Delete report log configurations.	write	-	-
aad:dashboard:get	Obtain report data and log configurations.	read	-	-
aad:dashboard:set	Modify report log configurations.	write	-	-
aad:domain:create	Add protected domain names.	write	domain *	g:EnterpriseProjectId
aad:domain:delete	Delete protected domain names.	write	domain *	g:EnterpriseProjectId
aad:domain:get	Query domain name details.	read	domain *	g:EnterpriseProjectId
aad:domain:list	Query the domain name list.	list	domain *	g:EnterpriseProjectId
aad:domain:put	Modify domain protection attributes.	write	domain *	g:EnterpriseProjectId
aad:forwardingRule:create	Add forwarding rules.	write	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:delete	Delete forwarding rules.	write	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:get	Query forwarding rules.	read	forwardingRule *	g:EnterpriseProjectId
aad:forwardingRule:list	Export forwarding rules.	list	forwardingRule *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aad:forwardingRule:put	Modify the back-to-source IP address permissions in the forwarding rule.	write	forwardingRule *	g:EnterpriseProjectId
aad:instance:create	Create an instance.	write	instance *	g:EnterpriseProjectId
aad:instance:get	Query instance attributes.	read	instance *	g:EnterpriseProjectId
aad:instance:list	Query the DB instance list.	list	instance *	g:EnterpriseProjectId
aad:instance:put	Modify instance attributes.	write	instance *	g:EnterpriseProjectId
aad:policy:create	Add protection rules.	write	policy *	g:EnterpriseProjectId
aad:policy:delete	Delete protection rules.	write	policy *	g:EnterpriseProjectId
aad:policy:get	Query protection rule details.	read	policy *	g:EnterpriseProjectId
aad:policy:list	Query protection rules.	list	policy *	g:EnterpriseProjectId
aad:policy:put	Modify protection rules.	write	policy *	g:EnterpriseProjectId
aad:quotas:get	Query protection specifications.	read	-	-
aad:whiteBlackIpRule:create	Add IP addresses to the blacklist or whitelist.	write	whiteBlackIpRule *	g:EnterpriseProjectId
aad:whiteBlackIpRule:delete	Delete IP addresses from the blacklist or whitelist.	write	whiteBlackIpRule *	g:EnterpriseProjectId
aad:whiteBlackIpRule:list	Query the protection blacklist and whitelist.	list	whiteBlackIpRule *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aad:protectedIp:put	Modify the labels of protected objects.	write	-	-
aad:protectedIp:list	Query the protected object list.	list	-	-
aad:package:put	Modify the protection package.	write	package *	-
aad:package:list	Query the protected IP address list.	list	package *	-
aad:block:put	Grant permission to unblock IP addresses.	write	-	-
aad:block:list	Query the blocked IP address list.	list	-	-
aad:block:get	Query blocking and unblocking information.	read	-	-

Each API of AAD usually supports one or more actions. **Table 5-134** lists the supported actions and dependencies.

Table 5-134 Actions and dependencies supported by AAD APIs

API	Action	Dependency
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	-

API	Action	Dependency
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	-
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	-

API	Action	Dependency
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	-
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	-

API	Action	Dependency
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	-
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	-

API	Action	Dependency
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	-
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	-

API	Action	Dependency
POST /v1/unblockservice/{domain_id}/unblock	aad:block:put	-
GET /v1/unblockservice/{domain_id}/block-list	aad:block:list	-
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	-

API	Action	Dependency
DELETE /v1/aad/whiteip	aad:policy:delete	-
POST /v1/aad/custom	aad:policy:put	-
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	-
GET /v1/aad/instances/{instance_id}/{ip}/ddos-statistics	aad:dashboard:get	-
GET /v1/aad/protected-domains/{domain_id}	aad:domain:get	-
GET /v1/aad/protected-domains	aad:domain:list	-
PUT /v1/aad/protected-domains/{domain_id}	aad:domain:put	-
POST /v1/aad/instances/{instance_id}/{ip}/rules/batch-create	aad:forwardingRule:create	-
POST /v1/aad/instances/{instance_id}/{ip}/rules/batch-delete	aad:forwardingRule:delete	-
GET /v1/aad/instances/{instance_id}/{ip}/rules	aad:forwardingRule:list	-
PUT /v1/aad/instances/{instance_id}/{ip}/rules/{rule_id}	aad:forwardingRule:put	-
GET /v1/aad/instances	aad:instance:list	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-135**, the resource URN must be specified in the SCP 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 SCP policy statements for AAD.

Table 5-135 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 SCP policies.

AAD can use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.8.2 Data Encryption Workshop (DEW)

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 permission 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 the OU or member account. Instead, the SCPs only determine what permissions are available for the member account or the member accounts under the OU.

This section describes the elements used by Organizations SCPs, which include actions, resources, and conditions.

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 a policy.

- The **Access Level** column describes how the action is classified (**List**, **Read**, or **Write**). This 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 does not contain any value (-), you must specify all resources (*) in your SCP statements.
  - If resource types are specified for this column, specify the resource URN in the statement that contains the action.
  - Required resources are marked with asterisks (*) in the table.

  For details about resource types defined by DEW, 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 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 resource types 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 DEW, see **Conditions**.

The following table describes the actions that you can define in SCP statements for DEW.

Table 5-136 Actions supported by KMS

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:create	Grant the permission to create KMS keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
kms:cmk:list	Grant the permission to view all KMS keys of a user.	list	KeyId *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:enable	Grant the permission to enable KMS keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:disable	Grant the permission to disable KMS keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:get	Grant the permission to view details about KMS keys.	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:createDataKey	Grant the permission to use KMS keys to generate data keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms:cmk:createDataKeyWithoutPlaintext	Grant the permission to use KMS keys to generate data keys that do not contain plaintext versions.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:encryptDataKey	Grant the permission to encrypt data keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms:cmk:decryptDataKey	Grant the permission to decrypt data keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:encryptData	Grant the permission to use a specified KMS key to encrypt small volumes of data.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:EncryptionAlgorithm • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms:cmk:decryptData	Grant the permission to use a specified KMS key to decrypt data.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:EncryptionAlgorithm • kms:RecipientAttestation • kms:RequestAlias • kms:ResourceAliases • kms:EncryptionContext
kms::generateRandom	Grant the permission to generate secure random strings.	write	-	kms:RecipientAttestation

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:sign	Grant the permission to generate digital signatures.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases
kms:cmk:verify	Grant the permission to use a specified KMS key to verify digital signatures.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:generateMac	Grant the permission to generate message verification codes.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:MessageType • kms:SigningAlgorithm • kms:RequestAlias • kms:ResourceAliases
kms:cmk:verifyMac	Grant the permission to use a specified KMS key to verify message verification codes.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:MacAlgorithm • kms:RequestAlias • kms:ResourceAliases

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:getPublicKey	Grant the permission to query the public key of KMS keys.	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• kms:RequestAlias • kms:ResourceAliases
kms::getVersions	Grant the permission to query the service version.	read	-	-
kms::getVersion	Grant the permission to query the API version of a service key.	read	-	-
kms::getInstance	Grant the permission to query the number of key instances of a user.	read	-	-
kms::getQuota	Grant the permission to query user quotas.	read	-	-
kms:cmk:scheduleKeyDeletion	Grant the permission to periodically delete KMS keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:ScheduleKeyDeletionPendingWindowInDays

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:cancelKeyDeletion	Grant the permission to cancel the scheduled deletion of KMS keys.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updateKeyAlias	Grant the permission to change the alias of a key.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updateKeyDescription	Grant the permission to change the key description.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:createGrant	Grant the permission to create grants for a specified key.	permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (* required)	Condition Key
			-	• kms:GranteePrincipalType • kms:GrantOperations • kms:GranteePrincipal • kms:RetiringPrincipal
kms:cmk:listGrants	Grant the permission to query the grant list of a specified key.	list	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms::listRetirableGrants	Grant the permission to query the retirable grant list of CMKs.	list	-	-
kms:cmk:retireGrant	Permission granted to retire a grant for a specified CMK.	permission_management	KeyId *	g:ResourceTag/<tag-key>
kms:cmk:revokeGrant	Grant the permission to cancel the grants of a specified key.	permission_management	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:getMaterial	Grant the permission to obtain key import parameters.	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:WrappingAlgorithm
kms:cmk:importMaterial	Grant the permission to import key materials.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:ExpirationTime
kms:cmk:deleteMaterial	Grant the permission to delete key materials.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:enableRotation	Grant the permission to enable rotation for a specified key.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updateRotation	Grant the permission to change the rotation period of a specified key.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:disableRotation	Grant the permission to disable rotation for a key.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:getRotation	Grant the permission to query the rotation status of a specified key.	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:createTag	Grant the permission to add tags to a specified key.	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
kms:cmk:createTags	Grant the permission to add or delete tags of a specified key in batches.	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
kms:cmk:listKeysByTag	Grant the permission to query a specified key instance.	list	KeyId *	-
kms:cmk:deleteTag	Grant the permission to delete a specified key tag.	tagging	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:cmk:getTags	Grant the permission to query a specified key tag.	read	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms::listAllTags	Grant the permission to query the tags of a specified key project.	list	-	-
kms:cmk:replicate	Grant the permission to copy a KMS key.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
kms:cmk:updatePrimaryRegion	Grant the permission to update the primary region.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	kms:PrimaryRegion

Action	Description	Access Level	Resource Type (* required)	Condition Key
kms:alias:create	Grant the permission to create an alias.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			alias *	-
kms:alias:delete	Grant the permission to delete an alias.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			alias *	-
kms:alias:list	Grant the permission to query the alias list.	list	-	-
kms:alias:associate	Grant the permission to associate an alias.	write	KeyId *	• kms:KeyOrigin • kms:KeySpec • kms:KeyUsage • kms:MultiRegionKeyType • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			alias *	-

Table 5-137 Actions supported by KPS

Action	Description	Access Level	Resource Type (* required)	Condition Key
kps:SSHKeyPair:create	Grant the permission to create and import SSH key pairs.	write	SSHKeyPair *	• kps:KmsKeyId • kps:Algorithm
kps:SSHKeyPair:delete	Grant the permission to delete SSH key pairs.	write	SSHKeyPair *	-
kps:SSHKeyPair:get	Grant the permission to query SSH key pair details.	read	SSHKeyPair *	-
kps:SSHKeyPair:list	Grant the permission to query the SSH key pair list.	list	SSHKeyPair *	-
kps:SSHKeyPair:update	Grant the permission to update the description of SSH key pairs.	write	SSHKeyPair *	-
kps:SSHKeyPair:bind	Grant the permission to bind a new SSH key pair to a VM.	write	SSHKeyPair *	-
kps::deleteFailedTask	Grant the permission to delete failed tasks.	write	-	-
kps:SSHKeyPair:unbind	Grant the permission to unbind an SSH key pair from a VM.	write	SSHKeyPair *	-
kps::getFailedTask	Grant the permission to query the information about failed tasks.	list	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
kps::getTask	Grant the permission to query the execution status of the current task.	list	-	-
kps::getRunningTask	Grant the permission to query the information about tasks that are being processed.	list	-	-
kps:SSHKeyPair:importPrivateKey	Grant the permission to import a private key to a key pair.	write	SSHKeyPair *	kps:KmsKeyId
kps:SSHKeyPair:exportPrivateKey	Grant the permission to export the private key from a key pair.	write	SSHKeyPair *	-
kps:SSHKeyPair:clearPrivateKey	Grant the permission to clear the private key of a key pair.	write	SSHKeyPair *	-

Table 5-138 Actions supported by CSMS

Action	Description	Access Level	Resource Type (* required)	Condition Key
csms:secret:create	Grant the permission to create and restore secrets.	write	secretName *	• csms:Type • csms:KmsKeyId

Action	Description	Access Level	Resource Type (* required)	Condition Key
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
csms:secret:delete	Grant the permission to delete secrets immediately.	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:update	Grant the permission to update secret metadata information.	write	secretName *	• csms:Type • csms:KmsKeyId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:get	Grant the permission to query and download secret information.	read	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:list	Grant the permission to query all secrets created by the current user in the current project.	list	secretName *	g:EnterpriseProjectId
csms:secret:createVersion	Grants the permission to create a new secret version in a specified secret.	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:getVersion	Grants permission to query the version information about a specified secret and its plaintext secret values.	read	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (* required)	Condition Key
csms:secret:listVersion	Grants the permission to query the version list of a specified secret.	list	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:createStage	Grant the permission to create secret version status.	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:getStage	Grant the permission to use the secret version status to query version information.	read	secretName *	• csms:Type • csms:VersionStage • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:updateStage	Grant the permission to update the secret version status.	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:deleteStage	Grant the permission to delete the state of a specified secret version.	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms::getSecretQuota	Grant the permission to query the secret quota of a specified project.	read	-	-
csms:secret:scheduleDeletion	Grant the permission to create a scheduled secret deletion task.	write	secretName *	• csms:Type • csms:RecoveryWindowInDays • g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (* required)	Condition Key
csms:secret:restoreSecret	Grant the permission to cancel a scheduled secret deletion task.	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:rotate	Grant the permission to rotate a secret.	write	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms:secret:getSecretsByTag	Grant the permission to return the secret list through tag filtering.	list	secretName *	-
csms:secret:batchCreateOrDeleteTags	Grant the permission to add or delete secret tags in batches.	tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
csms:secret:createTag	Grant the permission to add secret tags.	tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
csms:secret:deleteTag	Grant the permission to delete secret tags.	tagging	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	g:TagKeys

Action	Description	Access Level	Resource Type (* required)	Condition Key
csms:secret:listTags	Grant the permission to query secret tags.	list	secretName *	• csms:Type • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms::listProjectTags	Grant the permission to query all secret tag sets of a user in a specified project.	list	-	-
csms:secret:updateVersion	Grant the permission to update the validity period of a secret version.	write	secretName *	• csms:Type • csms:VersionId • g:EnterpriseProjectId • g:ResourceTag/<tag-key>
csms::createEvent	Grant the permission to create secret events.	write	-	-
csms::listEvents	Grant the permission to query all event notifications created by the current user in a project.	list	-	-
csms::getEvent	Grant the permission to query specified event notification information.	read	-	-
csms::updateEvent	Grant the permission to update the information of a specified event notification.	write	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
csms::deleteEvent	Grant the permission to immediately delete a specified event notification.	write	-	-
csms::listNotificationRecords	Grant the permission to query the triggered event notification records.	list	-	-
csms::listTasks	Grant the permission to query secret rotation tasks.	List	-	-

Table 5-139 Actions supported by Dedicated HSM

Action	Description	Access Level	Resource Type (* required)	Condition Key
dhsm:hsm:get	Grant the permission to query HSM details.	read	DHSM	-
dhsm:hsm:getJobInfo	Grant the permission to query task details.	read	DHSM	-
dhsm:cluster:getCsr	Grant the permission to download the certificate request file.	read	DHSM	-
dhsm:cluster:getCert	Grant the permission to query the cluster certificates.	read	DHSM	-
dhsm::getPreCreatedInfo	Grant the permission to query HSM resource information.	read	DHSM	-
dhsm:hsm:delete	Grant the permission to delete HSM details.	write	DHSM	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
dhsm:hsm:updateAlias	Grant the permission to update HSM information.	write	DHSM	-
dhsm:hsm:create	Grant the permission to create an HSM.	write	DHSM	-
dhsm:hsm:updateHsm	Grant the permission to update HSM information.	write	DHSM	-
dhsm:cluster:create	Grant the permission to create a cluster.	write	DHSM	-
dhsm:cluster:update	Grant the permission to update a cluster.	write	DHSM	-
dhsm:cluster:delete	Grant the permission to delete a cluster.	write	DHSM	-
dhsm:cluster:addVsm	Grant the permission to add HSMs in batches.	write	DHSM	-
dhsm:cluster:updateCert	Grant the permission to configure a certificate.	write	DHSM	-
dhsm:hsm:createInstallOrder	Grant the permission to create an installation order.	write	DHSM	-
dhsm:hsm:createOrder	Grant the permission to create an order.	write	DHSM	-
dhsm:hsm:inquiryResource	Grant the permission to query the price.	read	DHSM	-
dhsm:hsm:list	Grant the permission to obtain the HSM list.	list	DHSM	-
dhsm:cluster:list	Grant the permission to query a cluster.	list	DHSM	-
dhsm:hsm:listHsmsByTag	Grant the permission to query an HSM instance.	list	DHSM	-
dhsm:hsm:getHsmTags	Grant the permission to obtain the tag list.	list	DHSM	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
dhsm::listTags	Grant the permission to query all tags of an HSM.	list	DHSM	-
dhsm::listChargeSpecCode	Grant the permission to query the specification code.	list	DHSM	-
dhsm:hsm:createTags	Grant the permission to create or delete tags in batches.	tagging	DHSM	-
dhsm:hsm:createResourceTag	Grant the permission to create a resource tag.	tagging	DHSM	-
dhsm:hsm:deleteResourceTag	Grant the permission to delete a resource tag.	tagging	DHSM	-

DEW APIs usually support one or more actions. **Table 5-140**, **Table 5-141**, and **Table 5-142** describe the actions and dependencies supported by APIs, as well as the actions on which the API depends.

Table 5-140 Actions and dependencies supported by KMS APIs

API	Action	Dependent Permission
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	-

API	Action	Dependent Permission
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	-
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/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	-
POST /v1.0/{project_id}/kms/list-grants	kms:cmk:listGrants	-
POST /v1.0/{project_id}/kms/list-retirable-grants	kms::listRetirableGrants	-

API	Action	Dependent Permission
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}/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	-
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	-

Table 5-141 Actions and dependencies supported by CSMS APIs

API	Action	Dependencies
POST /v1/{project_id}/secrets	csms:secret:create	kms:cmk:createDataKey
POST /v1/{project_id}/secrets/{secret_name}/backup	csms:secret:get	• kms:cmk:createDataKey • kms:cmk:decryptDataKey • kms:cmk:list
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	-
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	-

API	Action	Dependencies
POST /v1/{project_id}/secrets/{secret_name}/rotate	csms:secret:rotate	• rds:password:update • kms:cmk:createGrant • kms:cmk:retireGrant
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	-
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	-

Table 5-142 Actions and dependencies supported by KPS APIs

API	Action	Dependencies
POST /v3/{project_id}/keypairs	kps:SSHKeyPair:create	• kms:cmk:createDataKey • kms:cmk:list
DELETE /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:delete	-
GET /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:get	-
GET /v3/{project_id}/keypairs	kps:SSHKeyPair:list	-
PUT /v3/{project_id}/keypairs/{keypair_name}	kps:SSHKeyPair:update	-
POST /v3/{project_id}/keypairs/associate	kps:SSHKeyPair:bind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/failed-tasks	kps::deleteFailedTask	-

API	Action	Dependencies
DELETE /v3/{project_id}/failed-tasks/{task_id}	kps::deleteFailedTask	-
POST /v3/{project_id}/keypairs/disassociate	kps:SSHKeyPair:unbind	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
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	• kms:cmk:createDataKey • kms:cmk:list
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	• ecs:cloudServers:createServers • ecs:cloudServers:deleteServers • ecs:cloudServers:showServer • ecs:cloudServers:attach • ecs:cloudServers:listServerBlockDevices • ecs:cloudServers:showServerBlockDevice • ecs:cloudServers:detachVolume • ecs:cloudServers:listServerInterfaces • ecs:cloudServers:listServersDetails • ecs:cloudServerFlavors:get • ecs:cloudServerQuotas:get • evs:types:get • evs:volumes:use • ims:images:get • vpc:subnets:list
DELETE /v3/{project_id}/keypairs/{keypair_name}/private-key	kps:SSHKeyPair:clearPrivateKey	-

Table 5-143 Actions and dependencies supported by Dedicated HSM APIs

API	Action	Dependent Permission
GET /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:get	-
GET /v1/{project_id}/dew/hsms/jobs/{job_id}	dhsm:hsm:getJobInfo	-
GET /v1/{project_id}/dew/clusters/{cluster_id}/csr	dhsm:cluster:getCsr	-

API	Action	Dependent Permission
GET /v1/{project_id}/dew/clusters/{cluster_id}/cert	dhsm:cluster:getCert	-
GET /v1/{project_id}/dew/resources	dhsm::getPreCreatedInfo	-
DELETE /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:delete	-
PUT /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:updateAlias	-
POST /v1/{project_id}/dew/hsms	dhsm:hsm:create	-
PUT /v1/{project_id}/dew/hsms/{hsm_id}	dhsm:hsm:updateHsm	-
POST /v1/{project_id}/dew/clusters	dhsm:cluster:create	-
PUT /v1/{project_id}/dew/clusters/{cluster_id}	dhsm:cluster:update	-
DELETE /v1/{project_id}/dew/clusters/{cluster_id}	dhsm:cluster:delete	-
POST /v1/{project_id}/dew/clusters/{cluster_id}/vsms	dhsm:cluster:addVsm	-
POST /v1/{project_id}/dew/clusters/{cluster_id}/cert	dhsm:cluster:updateCert	-
POST /v1/{project_id}/dew/install-order	dhsm:hsm:createInstallOrder	-
POST /v1/{project_id}/dew/order	dhsm:hsm:createOrder	-
POST /v1/dew/inquiry/resource	dhsm:hsm:inquiryResource	-
GET /v1/{project_id}/dew/hsms	dhsm:hsm:list	-
GET /v1/{project_id}/dew/clusters	dhsm:cluster:list	-
POST /v1/{project_id}/hsm/{resource_instances}/action	dhsm:hsm:listHsmsByTag	-
GET /v1/{project_id}/hsm/{resource_id}/tags	dhsm:hsm:getHsmTags	-
GET /v1/{project_id}/hsm/tags	dhsm::listTags	-
GET /v1/dew/spec-codes	dhsm::listChargeSpecCode	-

API	Action	Dependent Permission
POST /v1/{project_id}/hsm/{resource_id}/tags/action	dhsm:hsm:createTags	-
POST /v1/{project_id}/hsm/{resource_id}/tags	dhsm:hsm:createResourceTag	-
DELETE /v1/{project_id}/hsm/{resource_id}/tags/{key}	dhsm:hsm:deleteResourceTag	-

Resources

A resource type indicates the resources that an SCP policy applies to. Some actions describes in **Table 5-144** can be restricted to specific resources. If you specify a resource URN in an SCP statement, the SCPs only applies to the specified resources. If no resource URN is specified, the value of **Resource** will be * by default, and the SCP will apply to all resources. You can also set conditions in an SCP to specify the resource type.

The following table lists the resource types that you can define in SCP statements for DEW.

Table 5-144 Resource types supported by DEW

Resource Type	URN
KeyId	kms:<region>:<account-id>:KeyId:<cmk-id>
alias	kms:<region>:<account-id>:alias:<alias-name>
secretName	csms:<region>:<account-id>:secretName:<secret-name>
dhsm	dhsm:<region>:<account-id>:hsm:<hsm-id>
cluster	dhsm:<region>:<account-id>:cluster:<cluster-id>

Conditions

A Condition element lets you specify the conditions for an SCP to take effect. It contains condition keys and operators.

- The condition key 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, **DEW:**) apply only to operations of the corresponding service. For details, see **Table 5-145**.

  - 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 Operators.

The following table lists the condition keys that you can define in SCPs for DEW. You can use the condition keys to set conditions for detailed SCP statements.

NOTE

KPS does not support service-level condition keys in identity policies.

Table 5-145 Service-specific condition keys supported by DEW

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kms:EncryptionAlgorithm	string	Single-valued	Search for the encryption and decryption operations based on the value of encryption and decryption algorithms in the request.
kms:GranteePrincipalType	string	Single-valued	Search for the CreateGrant operations based on the authorization subject type in the request.
kms:GrantOperations	string	Multivalued	Search for the CreateGrant operations based on the operations that need to be authorized.
kms:GranteePrincipal	string	Single-valued	Search for the CreateGrant operations based on the authorized subjects in the authorization.
kms:KeyOrigin	string	Single-valued	Search for the API operations based on the **origin** attribute of the created or used KMS key.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kms:KeySpec	string	Single-valued	Search for the API operations based on the **key_spec** attribute of the created or used KMS key.
kms:KeyUsage	string	Single-valued	Search for the API operations based on the **key_usage** attribute of the created or used KMS key.
kms:MessageType	string	Single-valued	Search for the signing and signature verification operations based on the value of **message_type** in the request.
kms:RetiringPrincipal	string	Single-valued	Search for the CreateGrant operations based on value of **retiring_principal** in the grant.
kms:SigningAlgorithm	string	Single-valued	Search for the signing and verification operations based on the value of **signing_algorithm** in the request.
kms:ExpirationTime	date	Single-valued	Search for the ImportKeyMaterial operations based on the value of **expiration_time** in the request.
kms:WrappingAlgorithm	string	Single-valued	Search for the CreateParametersForImport operations based on the value of **wrapping_algorithm** in the request.
kms:RecipientAttestation	string	Single-valued	Search for the CreateDatakey, DecryptData, DecryptDatakey, and CreateRandom operations based on the value of platform configuration register (PCR) of the proof document in the request.
kms:MacAlgorithm	string	Single-valued	Search for the message authentication code generation or verification operations based on the value of **mac_algorithm** in the request.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
kms:RequestAlias	string	Single-valued	Filter access to API operations based on **key_id** in the request.
kms:ResourceAliases	string	Multivalued	Filter access to API operations based on **alias** of the KMS key.
kms:MultiRegionKeyType	string	Single-valued	Filter access to API operations based on **MultiRegionKeyType** in the KMS key field.
kms:PrimaryRegion	string	Single-valued	Filter access to API operations based on **primary_region** in the request.
kms:EncryptionContext	string	Single-valued	Filter access to API operations based on **additional_authenticated_data** in the request.
kms:ScheduleKeyDeletionPendingWindowInDays	numeric	Single-valued	Filter access to API operations based on **pending_days** in the request.
csms:Type	string	Single-valued	Filter access permissions by secret type.
csms:KmsKeyId	string	Single-valued	Filter access permissions by KMS key ID.
csms:VersionId	string	Single-valued	Filter access permissions by secret version ID.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
csms:VersionStage	string	Single-valued	Filter access permissions by secret version status.
csms:RecoveryWindowInDays	numeric	Single-valued	Filter access permissions by secret deletion waiting time.
kps:KmsKeyId	string	Single-valued	Filter access permissions by KMS key ID in the request.
kps:Algorithm	string	Single-valued	Filter access permissions by the algorithm used by the SSH key pair in the request.

5.10.8.3 Host Security Service (HSS)

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 permission 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.

- **Access Level** indicates how the action is classified. The value can be **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 resource URN in the **Resource** element of your statements.
  - Required resources are marked with asterisks (*) in the table.

  For details about the resource types defined by HSS, see **Resource**.

- 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 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 HSS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for HSS.

Table 5-146 Actions supported by HSS

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:host:addHostsGroup	Grants permission to create a server group.	write	host *	g:EnterpriseProjectId
hss:ars:addPWLPolicyHost	Grants permission to add servers to a whitelist policy.	write	host *	g:EnterpriseProjectId
hss:rasp:addRaspPolicy	Grants permission to add protection policies.	write	-	g:EnterpriseProjectId
hss:safetyReport:addSecurityReport	Grants permission to create or copy new reports.	write	-	g:EnterpriseProjectId
hss:wtp:addTimingOffConfigInfo	Grants permission to add the configuration of scheduled protection disabling.	write	host *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:wtp:addWtpHostProtectDirInfo	Grants permission to add protected directories.	write	host *	g:EnterpriseProjectId
hss:wtp:addWtpPrivilegedProcessInfo	Grants permission to add privileged processes.	write	host *	g:EnterpriseProjectId
hss:setting:changeAutoKillVirusStatus	Grants permission to enable or disable automatic program isolation and killing.	write	-	g:EnterpriseProjectId
hss:event:changeBlockedIp	Grants permissions for unblocking.	write	host *	g:EnterpriseProjectId
hss:setting:changeMalwareCollectStatus	Grants permission to enable or disable the sample collection for malware cloud scans.	write	-	g:EnterpriseProjectId
hss:ars:changePWLPolicy	Grants permission to modify whitelist policies.	write	-	g:EnterpriseProjectId
hss:ars:changePWLPolicyProcessStatus	Grants permission to mark the whitelist policy identification processes.	write	-	g:EnterpriseProjectId
hss:safetyReport:changeSecurityReport	Grants permission to modify reports.	write	-	g:EnterpriseProjectId
hss:ars:createPWLPolicy	Grants permission to create whitelist policies.	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:deletePWLPolicy	Grants permission to delete whitelist policies.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:ars:deletePWLPolicyHost	Grants permission to delete servers from a whitelist policy.	write	host *	g:EnterpriseProjectId
hss:antiransomware:deleteRansomwareDuplicationInfo	Grants permission to delete backup copies.	write	-	g:EnterpriseProjectId
hss:antiransomware:deleteRansomwareProtectionPolicy	Grants permission to delete protection policies.	write	-	g:EnterpriseProjectId
hss:rasp:deleteRaspPolicy	Grants permission to delete protection policies.	write	-	g:EnterpriseProjectId
hss:safetyReport:deleteSecurityReport	Grants permission to delete reports.	write	-	g:EnterpriseProjectId
hss:wtp:deleteTimingOffConfigInfo	Grants permission to delete the configuration of scheduled protection disabling.	write	host *	g:EnterpriseProjectId
hss:wtp:deleteWtpBackupHostInfo	Grants permission to delete the remote backup server.	write	host *	g:EnterpriseProjectId
hss:wtp:deleteWtpHostProtectDirInfo	Grants permission to delete protected directories.	write	host *	g:EnterpriseProjectId
hss:wtp:deleteWtpPrivilegedProcessInfo	Grants permission to delete privileged processes.	write	host *	g:EnterpriseProjectId
hss:setting:getAgentInstallScript	Grants permission to query the agent installation script.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:setting:getAlarmConfig	Grants permission to query alarm configurations.	read	-	g:EnterpriseProjectId
hss:rasp:getAppRaspSwitchStatus	Grants permission to query application protection status (enabled or disabled).	read	host *	g:EnterpriseProjectId
hss:setting:getAutoKillVirusStatus	Grants permission to query the automatic isolation and killing status of programs.	read	-	g:EnterpriseProjectId
hss:container:getContainerNodeStatistics	Grants permission to query container node protection overview statistics.	read	-	g:EnterpriseProjectId
hss:keyfile:getFileStatistic	Grants permission to obtain server file statistics.	read	-	g:EnterpriseProjectId
hss:setting:getMalwareCollectStatus	Grants permission to query the status of the sample collection configuration switch for malware cloud scans.	read	-	g:EnterpriseProjectId
hss:setting:getMalwareReminders	Grants permission to obtain prompt information configurations.	read	-	g:EnterpriseProjectId
hss:securitycheck:getManualSecurityCheckStatus	Grants permission to query the status and progress of manual health checks.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:overview:getOverviewAssetGroupsStatistics	Grants permission to obtain business group distribution statistics and identify regular, important, and core assets.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewAssetOsStatistics	Grants permission to obtain OS distribution statistics.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewAssetStatistics	Grants permission to obtain asset statistics, including servers, containers, and images.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewAttckMitre	Grants permission to investigate responses (ATT&CK attack path matrix).	read	-	g:EnterpriseProjectId
hss:overview:getOverviewDefenseStatistics	Grants permission to obtain proactive defense statistics.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewProtectionStatusStatistics	Grants permission to query the protection status of the current cloud loads.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewQuotaStatistics	Grants permission to obtain server security statistics.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewRiskLists	Grants permission to query the risk list.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:overview:getOverviewRiskManageStatistics	Grants permission to obtain risk management information, including risk trends and type statistics.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewRiskScore	Grants permission to query risk scores.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewRiskStatistics	Grants permission to query risk statistics, security risks, security alarms, and proactive defense.	read	-	g:EnterpriseProjectId
hss:overview:getOverviewTrialsStatistics	Grants permission to try server risk statistics.	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareBackupInfoByBackupId	Grants permission to query specified backup information.	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareHSSBackupPolicyInfo	Grants permission to query backup policy information.	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareBackupStatistics	Grants permission to query backup statistics.	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareProtectionStatistics	Grants permission to query protection statistics.	read	-	g:EnterpriseProjectId
hss:antiransomware:getRansomwareVaultInfo	Grants permission to query backup vault information.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:rasp:getRaspPolicyDetail	Grants permission to query protection policy details.	read	-	g:EnterpriseProjectId
hss:rasp:getRaspProtectStatistics	Grants permission to obtain protection data statistics.	read	-	g:EnterpriseProjectId
hss:wtp:getRaspSwitchStatus	Grants permission to query whether the dynamic WTP is enabled.	read	host *	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheck-Config	Grants permission to query security check schedules.	read	-	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheck-HostReport	Grants permission to query the security check report of a specified server.	read	host *	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheck-Overview	Grants permission to query the security check overview.	read	-	g:EnterpriseProjectId
hss:securitycheck:getSecurityCheck-Statistic	Grants permission to query security check statistics.	read	-	g:EnterpriseProjectId
hss:safetyReport:getSecurityReport	Grants permission to query the content of the security report.	read	-	g:EnterpriseProjectId
hss:safetyReport:getSecurityReport-Subscription	Grants permission to query the content of a report subscription.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:wtp:getTimingOffStatusInfo	Grants permission to query whether a protection configuration is in the scheduled disabling list.	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpDashboardProtectStatistics	Grants permission to query protection statistics.	read	-	g:EnterpriseProjectId
hss:wtp:getWtpDirectory	Grants permission to query the Tomcat bin directory for dynamic WTP.	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpDirectoryMonitorOnlyStatus	Grants permission to query the status of the monitoring-only switch.	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpPrivilegedProcessesChildStatus	Grants permission to display the trust status of privileged subprocesses.	read	host *	g:EnterpriseProjectId
hss:wtp:getWtpRemoteBackupHostInfo	Grants permission to query information about the remote backup server.	read	host *	g:EnterpriseProjectId
hss:setting:listAgentVersion	Grants permission to query agent versions.	list	-	g:EnterpriseProjectId
hss:container:listContainerNodes	Grants permission to query the container node list.	list	-	g:EnterpriseProjectId
hss:keyfile:listFileEvents	Grants permission to obtain the list of changed files.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:keyfile:listFileHostEventDetails	Grants permission to obtain details about change files on a server.	list	host *	g:EnterpriseProjectId
hss:keyfile:listFileHosts	Grants permission to obtain the ECS change list.	list	-	g:EnterpriseProjectId
hss:host:listHostGroups	Grants permission to query the server group list.	list	-	g:EnterpriseProjectId
hss:setting:listLoginCommonIp	Grants permission to query common login IP addresses.	list	-	g:EnterpriseProjectId
hss:setting:listLoginCommonLocation	Grants permission to query common login locations.	list	-	g:EnterpriseProjectId
hss:setting:listLoginWhiteIp	Grants permission to query the login IP address whitelist.	list	-	g:EnterpriseProjectId
hss:policy:listPolicyGroup	Grants permission to query the policy group list.	list	-	g:EnterpriseProjectId
hss:asset:listPortHost	Grants permission to query asset fingerprints - port - server list.	list	-	g:EnterpriseProjectId
hss:asset:listProcessesHost	Grants permission to query asset fingerprints - process - server list.	list	-	g:EnterpriseProjectId
hss:ars:listPWLEvent	Grants permission to query process whitelist events.	list	-	g:EnterpriseProjectId
hss:ars:listPwlPolicy	Grants permission to query the process whitelist policy list.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:ars:listPwlPolicyHost	Grants permission to query the servers associated with a process whitelist policy.	list	-	g:EnterpriseProjectId
hss:ars:listPwlPolicyProcess	Grants permission to query the process whitelist policy identification processes.	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareBackedupByHostId	Grants permission to query the vulnerability list.	list	host *	g:EnterpriseProjectId
hss:antiransomware:listRansomwareOperationLogsBy-VaultName	Grants permission to query the backup and restoration task list.	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareProtectionOptio-nalServer	Grants permission to query the servers under ransomware protection.	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareProtectionPolicy	Grants permission to query protection policies.	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareProtectionServer	Grants permission to query servers protected against ransomware.	list	-	g:EnterpriseProjectId
hss:rasp:listRaspCheckFeatureRule	Grants permission to query detection rules.	list	-	g:EnterpriseProjectId
hss:rasp:listRaspEvents	Grants permission to query application protection events.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:rasp:listRaspPolicies	Grants permission to query protection policies.	list	-	g:EnterpriseProjectId
hss:rasp:listRaspProtectionServers	Grants permission to query protected servers.	list	-	g:EnterpriseProjectId
hss:securitycheck:listSecurityCheck-HostReportHistory	Grants permission to query historical security check reports of a specified server.	list	host *	g:EnterpriseProjectId
hss:securitycheck:listSecurityCheck-HostResult	Grants permission to query the security check results of servers.	list	-	g:EnterpriseProjectId
hss:safetyReport:listSecurityReport	Grants permission to query the list on the report overview page.	list	-	g:EnterpriseProjectId
hss:safetyReport:listSecurityReport-tHistoryPeriod	Grants permission to query the statistical period list of historical reports.	list	-	g:EnterpriseProjectId
hss:safetyReport:listSecurityReport-SendingRecord	Grants permission to query report sending records.	list	-	g:EnterpriseProjectId
hss:wtp:listTimingOffConfigInfo	Grants permission to query the scheduled disabling list.	list	host *	g:EnterpriseProjectId
hss:setting:listTwoFactorLoginHost	Grants permission to query the list of servers with 2FA enabled.	list	-	g:EnterpriseProjectId
hss:wtp:listWtpBackupHostsInfo	Grants permission to query the remote backup server.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:wtp:listWtpHostProtectDirInfo	Grants permission to query protected directories.	list	host *	g:EnterpriseProjectId
hss:wtp:listWtpHostProtectHistor-yInfo	Grants permission to query the static WTP status of the server.	list	-	g:EnterpriseProjectId
hss:wtp:listWtpHostRaspProtectHis-toryInfo	Grants permission to query the dynamic WTP status of the server.	list	-	g:EnterpriseProjectId
hss:wtp:listWtpPrivilegedProcesse-sInfo	Grants permission to query privileged process configurations.	list	host *	g:EnterpriseProjectId
hss:wtp:listWtpProtectHost	Grants permission to query the protection list.	list	-	g:EnterpriseProjectId
hss:setting:modifyLoginCommonIp	Grants permission to add, edit, or delete common login IP addresses.	write	host *	g:EnterpriseProjectId
hss:setting:modifyLoginCommonLocation	Grants permission to add, edit, or delete common login locations.	write	host *	g:EnterpriseProjectId
hss:setting:modifyLoginWhiteIp	Grants permission to add, edit, or delete the login IP address whitelist.	write	host *	g:EnterpriseProjectId
hss:ars:operatePWLEvent	Grants permission to handle events.	write	-	g:EnterpriseProjectId
hss:ars:relearnPWLPolicy	Grants permission to relearn whitelist policies.	write	host *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:overview:resetOverviewRiskScore	Grants permission to reset risk scores and perform health checks again.	write	-	g:EnterpriseProjectId
hss:antiransomware:restoreRansomwareDuplicationInfo	Grants permission to back up and restore data.	write	-	g:EnterpriseProjectId
hss:safetyReport:sendSecurityReport	Grants permission to send security reports.	write	-	g:EnterpriseProjectId
hss:setting:setAlarmConfig	Grants permission to configure prompt information.	write	-	g:EnterpriseProjectId
hss:setting:setMalwareReminders	Grants permission to configure prompt information.	write	-	g:EnterpriseProjectId
hss:wtp:setRemoteWtpBackupInfo	Grants permission to enable or disable remote backup.	write	host *	g:EnterpriseProjectId
hss:wtp:setTimingOffSwitchInfo	Grants permission to set the status of the scheduled protection disabling.	write	host *	g:EnterpriseProjectId
hss:setting:setTwoFactorLoginConfig	Grants permission to configure 2FA login.	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpDirectoryMonitorOnlyStatus	Grants permission to configure the monitoring-only switch.	write	host *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:wtp:setWtpPrivilegedProcesse-sChildStatus	Grants permission to set the trust status of privileged subprocesses.	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpProtectionStatusInfo	Grants permission to enable or disable WTP.	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpProtectSwitch	Grants permission to enable or disable dynamic WTP.	write	host *	g:EnterpriseProjectId
hss:wtp:setWtpScheduledProtection-DateOffConfigInfo	Grants permission to configure the frequency and period for automatically disabling protection.	write	host *	g:EnterpriseProjectId
hss:securitycheck:startManualSecurityCheck	Grants permission to start a manual health check.	write	-	g:EnterpriseProjectId
hss:antiransomware:startRansomwareBackupSingle	Grants permission to enable the backup function for a single server.	write	host *	g:EnterpriseProjectId
hss:antiransomware:startRansomwareProtection	Grants permission to enable ransomware protection.	write	host *	g:EnterpriseProjectId
hss:antiransomware:startRansomwareProtectionSingle	Grants permission to enable ransomware protection for a single server.	write	host *	g:EnterpriseProjectId
hss:securitycheck:stopManualSecurityCheck	Grants permission to cancel a manual health check.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:antiransomware:stopRansomwareProtection	Grants permission to disable ransomware protection.	write	host *	g:EnterpriseProjectId
hss:container:switchContainerProtectStatus	Grants permission to switch the protection status.	write	host *	g:EnterpriseProjectId
hss:ars:switchPWLPolicyHost	Grants permission to enable or disable a server whitelist policy.	write	host *	g:EnterpriseProjectId
hss:rasp:switchRasp	Grants permission to enable or disable application protection.	write	host *	g:EnterpriseProjectId
hss:safetyReport:switchSecurityReportStatus	Grants permission to enable or disable security reports.	write	-	g:EnterpriseProjectId
hss:wtp:switchWtpHostProtectDirInfo	Grants permission to enable or disable directory protection.	write	host *	g:EnterpriseProjectId
hss:host:uninstallAgents	Grants permission to uninstall the agent.	write	host *	g:EnterpriseProjectId
hss:setting:updateAlarmConfig	Grants permission to configure alarm configurations.	write	-	g:EnterpriseProjectId
hss:antiransomware:updateRansomwareBackupPolicyInfo	Grants permission to modify backup policies.	write	-	g:EnterpriseProjectId
hss:antiransomware:updateRansomwareProtectionPolicy	Grants permission to modify protection policies.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:rasp:updateRaspPolicy	Grants permission to modify protection policies.	write	-	g:EnterpriseProjectId
hss:securitycheck:updateSecurityCheckConfig	Grants permission to modify security check schedules.	write	-	g:EnterpriseProjectId
hss:wtp:updateTimingOffConfigInfo	Grants permission to modify the configuration of scheduled protection disabling.	write	host *	g:EnterpriseProjectId
hss:wtp:updateWtpBackupHostInfo	Grants permission to add or modify a remote backup server.	write	host *	g:EnterpriseProjectId
hss:wtp:updateWtpDirectoryInfo	Grants permission to modify the Tomcat bin directory of dynamic WTP.	write	host *	g:EnterpriseProjectId
hss:wtp:updateWtpHostProtectDirInfo	Grants permission to modify protected directories.	write	host *	g:EnterpriseProjectId
hss:wtp:updateWtpPrivilegedProcessInfo	Grants permission to modify privileged processes.	write	host *	g:EnterpriseProjectId
hss:asset:addValuesLevel	Grants permission to configure asset management - server management - asset importance.	write	host *	g:EnterpriseProjectId
hss:asset:batchModifyPortStatus	Grants permission to change port status.	write	host *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:deleteToolConditionHistory	Grants permission to clear the search records of tools (operation tool).	write	-	g:EnterpriseProjectId
hss:asset:executeTool	Grants permission to perform search with tools (operation tools).	write	-	g:EnterpriseProjectId
hss:asset:getAccountTop	Grants permission to obtain asset management - overview - top accounts.	read	-	g:EnterpriseProjectId
hss:asset:getAgentStatisticsStatus	Grants permission to obtain asset management - overview - asset status - server agent status.	read	-	g:EnterpriseProjectId
hss:asset:getAssetStatistic	Grants permission to obtain asset statistics, including accounts, ports, and processes.	read	-	g:EnterpriseProjectId
hss:asset:getAssetType	Grants permission to obtain asset management - overview - asset status - asset distribution.	read	-	g:EnterpriseProjectId
hss:asset:getAutoLaunchTop	Grants permission to obtain asset management - overview - top auto-started items.	read	-	g:EnterpriseProjectId
hss:asset:getCommonPort	Grants permission to display details about a port.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:getContainerProtectionStatus	Grants permission to obtain asset management - overview - asset status - container protection status.	read	-	g:EnterpriseProjectId
hss:asset:getCoreConfFileTop	Grants permission to obtain asset management - overview - top key configurations.	read	-	g:EnterpriseProjectId
hss:asset:getEnvironmentTop	Grants permission to obtain asset management - overview - top environment variables.	read	-	g:EnterpriseProjectId
hss:asset:getHostAssetManualCollectStatus	Grants permission to obtain the status of the API for immediately collecting the asset fingerprints of a server.	read	host *	g:EnterpriseProjectId
hss:asset:getHostProtectionStatus	Grants permission to obtain asset management - overview - asset status - agent status.	read	-	g:EnterpriseProjectId
hss:asset:getJarPackageTop	Grants permission to obtain asset management - overview - top JAR packages.	read	-	g:EnterpriseProjectId
hss:asset:getKernelModuleTop	Grants permission to obtain asset management - overview - top kernel modules.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:getOsStatisticsInfo	Grants permission to obtain asset management - overview - asset status - OS statistics.	read	-	g:EnterpriseProjectId
hss:asset:getPorcessTop	Grants permission to obtain asset management - overview - top processes.	read	-	g:EnterpriseProjectId
hss:asset:getPortTop	Grants permission to obtain asset management - overview - top ports.	read	-	g:EnterpriseProjectId
hss:asset:getQuotaStatisticsInfo	Grants permission to obtain asset management - overview - asset status - protection quota statistics.	read	-	g:EnterpriseProjectId
hss:asset:getSoftwareTop	Grants permission to obtain asset management - overview - top software.	read	-	g:EnterpriseProjectId
hss:asset:getWebAppAndServiceTop	Grants permission to obtain asset management - overview - top web apps and services.	read	-	g:EnterpriseProjectId
hss:asset:getWebAppTop	Grants permission to obtain asset management - overview - top web applications.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:getWebFrameworkTop	Grants permission to obtain asset management - overview - top web frameworks.	read	-	g:EnterpriseProjectId
hss:asset:getWebServiceTop	Grants permission to obtain asset management - overview - top web services.	read	-	g:EnterpriseProjectId
hss:asset:getWebSiteTop	Grants permission to obtain asset management - overview - top websites.	read	-	g:EnterpriseProjectId
hss:asset:listAppChangeHistories	Grants permission to obtain asset fingerprints – software information – operation history.	list	-	g:EnterpriseProjectId
hss:asset:listApps	Grants permission to obtain asset fingerprints of a single server – software.	list	-	g:EnterpriseProjectId
hss:asset:listAppStatistics	Grants permission to obtain asset fingerprints – software information.	list	-	g:EnterpriseProjectId
hss:asset:listAutoLaunchChangeHistories	Grants permission to obtain asset fingerprints - auto-started items - change history.	list	-	g:EnterpriseProjectId
hss:asset:listAutoLaunchs	Grants permission to obtain asset fingerprints of a server - auto-started items.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:listAutoLaunchStatistics	Grants permission to obtain asset fingerprints - auto-start items.	list	-	g:EnterpriseProjectId
hss:asset:listCoreConfFileHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of key configuration files.	list	-	g:EnterpriseProjectId
hss:asset:listCoreConfFileInfo	Grants permission to obtain asset management - server management - fingerprint type - key configurations.	list	host *	g:EnterpriseProjectId
hss:asset:listCoreConfFileStatistics	Grants permission to obtain asset management - asset fingerprints - key configuration file navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listEnvironmentHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of key environment variables (on the right of asset fingerprints).	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:listEnvironmentInfo	Grants permission to obtain asset management - server management - fingerprint type - environment variables.	list	host *	g:EnterpriseProjectId
hss:asset:listEnvironmentStatistics	Grants permission to obtain asset management - asset fingerprints - environment variable file navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listJarPackageHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of JAR packages.	list	-	g:EnterpriseProjectId
hss:asset:listJarPackageInfo	Grants permission to obtain asset management - server management - fingerprint type - JAR packages.	list	host *	g:EnterpriseProjectId
hss:asset:listJarPackageStatistics	Grants permission to obtain asset management - asset fingerprints - JAR package navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listKernelModuleHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of kernel modules.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:listKernelModuleInfo	Grants permission to obtain asset management - server management - fingerprint type - kernel modules.	list	host *	g:EnterpriseProjectId
hss:asset:listKernelModuleStatistics	Grants permission to obtain asset management - asset fingerprints - kernel module navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listPorts	Grants permission to obtain single-server asset fingerprint (open port information).	list	host *	g:EnterpriseProjectId
hss:asset:listPortStatistics	Grants permission to obtain asset fingerprints (open port information).	list	-	g:EnterpriseProjectId
hss:asset:listProcesses	Grants permission to obtain the process list.	list	host *	g:EnterpriseProjectId
hss:asset:listProcessStatistics	Grants permission to obtain asset fingerprints (process information).	list	-	g:EnterpriseProjectId
hss:asset:listResult	Grants permission to obtain execution results (operation tools).	list	-	g:EnterpriseProjectId
hss:asset:listTool	Grants permission to obtain the tool list (operation tools).	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:listToolConditionHistory	Grants permission to obtain the search records of tools (operation tools).	list	-	g:EnterpriseProjectId
hss:asset:listUserChangeHistories	Grants permission to obtain the account change history.	list	-	g:EnterpriseProjectId
hss:asset:listUserGroup	Grants permission to obtain the user group list.	list	-	g:EnterpriseProjectId
hss:asset:listUsers	Grants permission to obtain the account list of assets.	list	-	g:EnterpriseProjectId
hss:asset:listUserStatistics	Grants permission to obtain asset fingerprints - software information.	list	-	g:EnterpriseProjectId
hss:asset:listWebAppAndServices	Grants permission to obtain asset management - asset fingerprints - web app and service assets on the right.	list	-	g:EnterpriseProjectId
hss:asset:listWebAppAndServiceStatistics	Grants permission to obtain asset management - asset fingerprints - web app and service navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listWebAppHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of web applications.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:listWebAppInfo	Grants permission to obtain asset management - server management - fingerprint type - web applications.	list	host *	g:EnterpriseProjectId
hss:asset:listWebAppStatistics	Grants permission to obtain asset management - asset fingerprints - web application navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listWebFrameworkHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of web frameworks.	list	-	g:EnterpriseProjectId
hss:asset:listWebFrameworkInfo	Grants permission to obtain asset management - server management - fingerprint type - web frameworks.	list	host *	g:EnterpriseProjectId
hss:asset:listWebFrameworkStatistics	Grants permission to obtain asset management - asset fingerprints - web framework navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listWebServiceHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of web servers.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:asset:listWebServiceInfo	Grants permission to obtain asset management - server management - fingerprint type - web services.	list	host *	g:EnterpriseProjectId
hss:asset:listWebServiceStatistics	Grants permission to obtain asset management - asset fingerprints - web services navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:listWebSiteHostInfo	Grants permission to obtain asset management - asset fingerprints - the server list of websites.	list	-	g:EnterpriseProjectId
hss:asset:listWebSiteInfo	Grants permission to obtain asset management - server management - fingerprint type - websites.	list	host *	g:EnterpriseProjectId
hss:asset:listWebSiteStatistics	Grants permission to obtain asset management - asset fingerprints - website navigation tree on the left.	list	-	g:EnterpriseProjectId
hss:asset:runHostAssetManualCollect	Grants permission to immediately collect the asset fingerprints of a server.	write	host *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:baseline:addSecurityCheckPolicyGroup	Grants permission to create a configuration detection policy.	write	-	g:EnterpriseProjectId
hss:baseline:changeCheckRuleState	Grants permission to ignore, unignore, repair, and verify failed configuration check items.	write	baseline *	g:EnterpriseProjectId
hss:baseline:deleteSecurityCheckPolicyGroup	Grants permission to delete a specified configuration detection policy.	write	-	g:EnterpriseProjectId
hss:baseline:exportSecurityCheckReport	Grants permission to export the configuration detection report.	list	-	g:EnterpriseProjectId
hss:baseline:getBaselineOverview	Grants permission to query baseline check statistics.	read	-	g:EnterpriseProjectId
hss:baseline:getBaselineScanStatus	Grants permission to query the progress of a baseline check task.	read	-	g:EnterpriseProjectId
hss:baseline:getBaselineStatistic	Grants permission to query baseline check statistics, including weak passwords, password complexity, and configuration detection.	read	-	g:EnterpriseProjectId
hss:baseline:getCheckRuleDetail	Grants permission to query the check report of a configuration check item.	read	baseline *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:baseline:getCheckRuleFixFailDetail	Grants permission to query the cause of the check item repair failure.	read	baseline *	g:EnterpriseProjectId
hss:baseline:getDefaultSecurityCheckPolicy	Grants permission to query the default baseline of a configuration detection policy.	read	-	g:EnterpriseProjectId
hss:baseline:getDefaultSecurityCheckPolicyDetails	Grants permission to query detailed baseline check items.	read	-	g:EnterpriseProjectId
hss:baseline:getRiskConfigDetail	Grants permission to query the check result of a specified security configuration item.	read	-	g:EnterpriseProjectId
hss:baseline:listCheckRuleHost	Grants permission to query servers covered by a configuration check item.	list	baseline *	g:EnterpriseProjectId
hss:baseline:listPasswordComplexity	Grants permission to query the password complexity policy check report.	list	-	g:EnterpriseProjectId
hss:baseline:listRiskConfigCheckRules	Grants permission to query the check item list of a specified security configuration item.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:baseline:listRiskConfigHosts	Grants permission to query servers affected by a specified security configuration item.	list	-	g:EnterpriseProjectId
hss:baseline:listRiskConfigs	Grants permission to query the server security configuration check result list of a tenant.	list	-	g:EnterpriseProjectId
hss:baseline:listSecurityCheckPolicyGroup	Grants permission to query the list of configuration detection policy groups.	list	-	g:EnterpriseProjectId
hss:baseline:listWeakPasswordUsers	Grants permission to query the weak password detection results.	list	-	g:EnterpriseProjectId
hss:baseline:runBaselineDetect	Grants manual detection permissions. Performs configuration detection and weak password detection on the servers specified in the policy.	write	-	g:EnterpriseProjectId
hss:baseline:updateSecurityCheckPolicyGroup	Grants permission to modify a specified configuration detection policy.	write	-	g:EnterpriseProjectId
hss:event:addLoginWhiteList	Grants permission to add a login whitelist.	write	-	g:EnterpriseProjectId
hss:event:batchChangeEvent	Grants permission to handle alarm events in batches.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:event:changeEvent	Grants permission to handle alarm events.	write	event *	g:EnterpriseProjectId
hss:event:changeIsolatedFile	Grants permission to restore isolated files.	write	host *	g:EnterpriseProjectId
hss:event:exportAlarmWhiteList	Grants permission to export the alarm whitelist.	list	-	g:EnterpriseProjectId
hss:event:exportEmergency	Grants permissions to export emergency malware interfaces.	list	-	g:EnterpriseProjectId
hss:event:getEmergencyStatistics	Grants permission to obtain emergency event statistics.	read	-	g:EnterpriseProjectId
hss:event:getEventAttackTag	Grants permission to query the list of attack ID distribution statistics.	read	-	g:EnterpriseProjectId
hss:event:getEventSeverity	Grants permission to query the list of threat level statistics.	read	-	g:EnterpriseProjectId
hss:event:getEventStatistics	Grants permission to query alarm event statistics.	read	-	g:EnterpriseProjectId
hss:event:getMalwareInfo	Grants permission to obtain the list of unexpected malicious program events.	read	event *	g:EnterpriseProjectId
hss:event:handleMalwareEvent	Grants permission to handle malware.	write	event *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:event:importAlarmWhiteList	Grants permission to import an alarm whitelist.	write	-	g:EnterpriseProjectId
hss:event:isolateOperateEmergency	Grants permission to enable or disable the isolation box.	write	-	g:EnterpriseProjectId
hss:event:listAlarmWhiteList	Grants permission to query the alarm whitelist.	list	-	g:EnterpriseProjectId
hss:event:listBlockedIp	Grants permission to query the list of blocked IP addresses.	list	-	g:EnterpriseProjectId
hss:event:listEventOperates	Grants permission to query the handling types supported by events.	list	-	g:EnterpriseProjectId
hss:event:listEventTopRisk	Grants permission to query the list of top 10 event type statistics.	list	-	g:EnterpriseProjectId
hss:event:listEventType	Grants permission to query the list of event type statistics.	list	-	g:EnterpriseProjectId
hss:event:listFileIsolateList	Grants permission to obtain the list of files isolated due to unexpected malware events.	list	-	g:EnterpriseProjectId
hss:event:listIsolatedFile	Grants permission to query the isolated file list.	list	-	g:EnterpriseProjectId
hss:event:listLoginWhiteList	Grants permission to query the login whitelist.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:event:listMalware	Grants permission to obtain the list of unexpected malicious program events.	list	-	g:EnterpriseProjectId
hss:event:listSecurityEvents	Grants permission to query the intrusion event list.	list	-	g:EnterpriseProjectId
hss:event:recoverIsolateFile	Grants permission to restore the file isolation box.	write	-	g:EnterpriseProjectId
hss:event:removeAlarmWhiteList	Grants permission to delete an alarm whitelist.	write	-	g:EnterpriseProjectId
hss:event:removeLoginWhiteList	Grants permission to delete a login whitelist.	write	-	g:EnterpriseProjectId
hss:host:associateHostAssetValue	Grants permission to associate asset importance.	write	host *	g:EnterpriseProjectId
hss:host:associateHostsGroup	Grants permission to allocate servers to a server group.	write	host *	g:EnterpriseProjectId
hss:host:batchInstallAgent	Grants permission to install agents in batches.	write	host *	g:EnterpriseProjectId
hss:host:changeHostsGroup	Grants permission to edit a server group.	write	-	g:EnterpriseProjectId
hss:host:deleteHostsGroup	Grants permission to delete a server group.	write	-	g:EnterpriseProjectId
hss:host:getHostsStatistics	Grants permission to collect server statistics.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:host:listFirewallStatus	Grants permission to query the firewall status of a server.	read	host *	g:EnterpriseProjectId
hss:host:listHostGroupAssetValue	Grants permission to query the list of server groups by asset importance.	list	-	g:EnterpriseProjectId
hss:host:listHostsRisk	Grants permission to obtain ECS risk status.	read	host *	g:EnterpriseProjectId
hss:host:listHostStatus	Grants permission to query the list of protected servers.	list	-	g:EnterpriseProjectId
hss:host:listHostsUpgrade	Grants permission to obtain the agent upgrade status of a server.	read	host *	-
			-	g:EnterpriseProjectId
hss:host:manualCheckVul	Grants permission to manually detect vulnerabilities.	write	-	g:EnterpriseProjectId
hss:host:switchFirewallStatus	Grants permission to modify the firewall authorization status.	write	host *	g:EnterpriseProjectId
hss:host:switchHostsProtectStatus	Grants permission to switch the protection status.	write	host *	g:EnterpriseProjectId
hss:host:upgradeAgent	Grants permission to upgrade the agent from 1.0 to 2.0.	write	host *	-
			-	g:EnterpriseProjectId
hss:host:upgradeAgents	Grants permission to upgrade the agent.	write	host *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:batchScanLocalImage	Grants permission to perform local image scanning.	write	-	g:EnterpriseProjectId
hss:image:batchScanPrivateImage	Grants permission to scan images in private image repositories in batches.	write	-	g:EnterpriseProjectId
hss:image:getImageFilesStat	Grants permission to query image file statistics.	read	-	g:EnterpriseProjectId
hss:image:getImageLocalVulOverview	Grants permission to query local vulnerabilities.	read	-	g:EnterpriseProjectId
hss:image:getImageVulOverview	Grants permission to query repository vulnerabilities.	read	-	g:EnterpriseProjectId
hss:image:listCfgCheckAffectedImage	Grants permission to query the list of images affected by a tenant image that failed baseline checks.	list	-	g:EnterpriseProjectId
hss:image:listGlobalCfgCheck	Grants permission to query container image baseline inspection results.	list	-	g:EnterpriseProjectId
hss:image:listGlobalMalware	Grants permission to query the list of malicious tenant files.	list	-	g:EnterpriseProjectId
hss:image:listGlobalVul	Grants permission to query vulnerability details about a tenant image.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:listImageApps	Grants permission to query the image software list.	list	-	g:EnterpriseProjectId
hss:image:listImageAppVul	Grants permission to query the software vulnerability list.	list	-	g:EnterpriseProjectId
hss:image:listImageCfgCheck	Grants permission to query configuration baseline check results of an image.	list	-	g:EnterpriseProjectId
hss:image:listImageFiles	Grants permission to query the list of image files that have no owners.	list	-	g:EnterpriseProjectId
hss:image:listImageLocal	Grants permission to query the local image list.	list	-	g:EnterpriseProjectId
hss:image:listImageMalware	Grants permission to query the list of malicious image files.	list	-	g:EnterpriseProjectId
hss:image:listImageNamespace	Grants permission to query the namespace of an image.	list	-	g:EnterpriseProjectId
hss:image:listImageRepository	Grants permission to query the list of images in a private image repository.	list	-	g:EnterpriseProjectId
hss:image:listImageVul	Grants permission to query image vulnerability details.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:listInstanceImageVul	Grants permission to query vulnerability details about enterprise images.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageApp	Grants permission to query the local software image list.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageAppVuls	Grants permission to query the vulnerability list of a piece of software in a local image.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageContainers	Grants permission to query the container information about a local image.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageHosts	Grants permission to query the server information about a local image.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageMalware	Grants permission to query malicious file information about local images.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageVuls	Grants permission to query vulnerability information about a local image.	list	-	g:EnterpriseProjectId
hss:image:listLocalVulRepoImage	Grants permission to query details about images and containers affected by local image vulnerabilities.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:listPrivateImageRepository	Grants permission to query the list of images in a private image repository.	list	-	g:EnterpriseProjectId
hss:image:listSharedImageRepository	Grants permission to query the list of images in the shared image repository.	list	-	g:EnterpriseProjectId
hss:image:listVulCve	Grants permission to query CVE details about a vulnerability.	list	-	g:EnterpriseProjectId
hss:image:listVulRepoImage	Grants permission to query details about images in the image repository affected by a vulnerability.	list	-	g:EnterpriseProjectId
hss:image:runImageScan	Grants permission to scan images.	write	-	g:EnterpriseProjectId
hss:image:runImageSynchronizeTask	Grants permission to synchronize the free image list from SWR.	write	-	g:EnterpriseProjectId
hss:image:runSwrImageScan	Grants permission to update and scan SWR images and to access SWR.	write	-	g:EnterpriseProjectId
hss:image:sharedImageSynchronization	Grants permission to update images shared from SWR.	write	-	g:EnterpriseProjectId
hss:policy:addPolicyGroup	Grants permission to copy server policy groups.	write	policy *	g:EnterpriseProjectId
hss:policy:associatePolicyGroup	Grants permission to deploy a policy.	write	policy *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
			host *	g:EnterpriseProjectId
hss:policy:changePolicyDetail	Grants permission to modify a policy.	write	policy *	g:EnterpriseProjectId
hss:policy:changePolicyGroup	Grants permission to modify policy groups.	write	policy *	g:EnterpriseProjectId
hss:policy:deletePolicyGroup	Grants permission to delete policy groups.	write	policy *	g:EnterpriseProjectId
hss:policy:getPolicyDetail	Grants permission to query details about a specified policy.	read	policy *	g:EnterpriseProjectId
hss:policy:listPolicyGroupDetail	Grants permission to query the policy information list of a policy group.	list	policy *	g:EnterpriseProjectId
hss:quota:addResourceInstanceTag	Grants permission to add tags to a resource.	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:batchCreateTags	Grants permission to create tags in batches.	write	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:batchDeleteTags	Grants permission to delete tags in batches.	write	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:cancelHostsQuota	Grants permission to unbind quotas.	write	-	-
hss:quota:changeTmsResourceTagInfo	Grants permission to add or delete resource tags in batches.	write	-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:quota:countResourceInstances	Grants permission to query the number of purchased resources by tag.	list	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:dealOrder	Grants permission to subscribe to HSS.	write	-	-
hss:quota:deleteResourceInstance-Tag	Grants permission to delete tags from a resource.	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:filterResourceInstanceList	Grants permission to search for purchased resources by tag.	list	-	• g:RequestTag/<tag-key> • g:TagKeys
hss:quota:getResourceInstanceTag	Grants permission to query tags of a resource.	read	-	-
hss:quota:getResourceQuotas	Grants permission to query quota information.	read	-	-
hss:quota:getTmsResourceTagsInfo	Grants permission to query resource tags.	read	-	-
hss:quota:listProjectTags	Grants permission to query all used tags in the current project.	list	-	-
hss:quota:listQuotasDetail	Grants permission to query quota details.	list	-	-
hss:quota:listResourceIds	Grants permission to query quota IDs in batches.	list	-	-
hss:quota:listTmsResourceInstance-sInfo	Grants permission to query resource instances.	list	-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:quota:upgradeOrder	Grants permission to change specifications.	write	-	-
hss:vulnerability:changeVulStatus	Grants permission to modify the status of a vulnerability.	write	host *	g:EnterpriseProjectId
hss:vulnerability:exportEmergencyVulnerabilities	Grants permission to export emergency vulnerabilities.	list	-	g:EnterpriseProjectId
hss:vulnerability:exportVulsList	Grants permission to export information about vulnerabilities and their affected servers.	list	-	g:EnterpriseProjectId
hss:vulnerability:getCmsVulDetail	Grants permission to query basic information about the Web-CMS vulnerabilities.	read	-	g:EnterpriseProjectId
hss:vulnerability:getEmergencySummary	Grants permission to query the event overview.	read	-	g:EnterpriseProjectId
hss:vulnerability:getEmergencyVulDetail	Grants permission to query vulnerability details in events.	read	-	g:EnterpriseProjectId
hss:vulnerability:getLinuxVulDetail	Grants permission to query basic information about Linux vulnerabilities.	read	-	g:EnterpriseProjectId
hss:vulnerability:getVulCheckStatus	Grants permission to query the status of server vulnerability scanning.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:getVulSummary	Grants permission to query vulnerability statistics.	read	-	g:EnterpriseProjectId
hss:vulnerability:getWindosVulDetail	Grants permission to query basic information about Windows vulnerabilities.	read	-	g:EnterpriseProjectId
hss:vulnerability:getWindowsVulNum	Grants permission to query the number of Windows vulnerabilities on a server.	list	-	g:EnterpriseProjectId
hss:vulnerability:listEmergencyVul	Grants permission to query vulnerabilities in events.	list	-	g:EnterpriseProjectId
hss:vulnerability:listHostVuls	Grants permission to query vulnerability information about a single server.	list	host *	g:EnterpriseProjectId
hss:vulnerability:listHostVulSummary	Grants permission to query server statistics and top 5 risky servers.	list	-	g:EnterpriseProjectId
hss:vulnerability:listTopVulSummary	Grants permission to query top 5 vulnerabilities.	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHosts	Grants permission to query ECSs affected by a specific vulnerability.	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulnerabilities	Grants permission to query the vulnerability list.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:listVulRepairFailed-Detail	Grants permission to query information about vulnerability fixing failures.	list	host *	g:EnterpriseProjectId
hss:vulnerability:listVulTypeSummary	Grants permission to query vulnerability type distribution.	list	-	g:EnterpriseProjectId
hss:vulnerability:operateEmergency	Grants permission to operate vulnerabilities in events.	write	-	g:EnterpriseProjectId
hss:host:getScanStatus	Grants permission to query the manual scan status.	read	host *	g:EnterpriseProjectId
hss:host:setManualDetect	Grants permission to deliver a manual scan.	write	host *	g:EnterpriseProjectId
hss::getTrustServiceStatus	Grants permission to obtain the status of trusted services.	read	-	-
hss::enableTrustService	Grants permission to enable trusted services.	permission_management	-	-
hss::validateAdmin	Grants permission to check whether the current account is an administrator account (organization administrator or agency administrator).	tagging	-	-
hss::listAccounts	Grants permission to display the account list.	list	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss::batchAddAccounts	Grant permission to add accounts in batches.	write	-	-
hss::deleteAccount	Grants permission to delete accounts.	write	-	-
hss::listOrganizationTree	Grants permission to display the account tree structure.	list	-	-
hss::listDelegatedAccounts	Grants permission to query the tree structure of delegated accounts.	list	-	-
hss:antiransomware:listBackupVaults	Grants permission to query the backup vault list.	list	-	g:EnterpriseProjectId
hss:antiransomware:listRansomwareProtectionNodes	Grants permission to query servers protected against ransomware.	list	-	g:EnterpriseProjectId
hss:antiransomware:getBackupsStatistics	Grants permission to query backup statistics.	list	-	g:EnterpriseProjectId
hss:antiransomware:startSingleBack-up	Grants permission to enable the backup function for a single server.	write	host *	-
			-	g:EnterpriseProjectId
hss:antiransomware:getBackupPolicyInfo	Grants permission to query a backup policy.	read	-	g:EnterpriseProjectId
hss:hostGroup:getOutsideGroupSta-tus	Grants permission to query whether data center server groups can be created.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:hostGroup:getOutsideHostGroup	Grants permission to query off-cloud data center server groups.	read	-	g:EnterpriseProjectId
hss:hostGroup:addOutsideHostGroup	Grants permission to create off-cloud data center server groups.	write	-	g:EnterpriseProjectId
hss:hostGroup:changeOutsideHostGroup	Grants permission to edit off-cloud data center server groups.	write	-	g:EnterpriseProjectId
hss:images:listImageTag	Grant the permission to query the image tag version list.	list	-	g:EnterpriseProjectId
hss:images:listImageSensitive	Grants permission to query sensitive image information.	list	-	g:EnterpriseProjectId
hss:images:getFilePathWhiteDetail	Grants permission to query the sensitive information file path whitelist of images.	read	-	g:EnterpriseProjectId
hss:images:changeFilePathWhiteDetail	Grants permission to modify the sensitive information file path whitelist of images.	write	-	g:EnterpriseProjectId
hss:images:changeSensitiveInfo	Grants permission to perform operations on sensitive information.	write	-	g:EnterpriseProjectId
hss:event:listTopEventType	Grants permission to query the statistics about the top 5 events.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:getVulScanPolicy	Grants permission to query a vulnerability scan policy.	read	-	-
hss:vulnerability:changeVulScanPolicy	Grants permission to modify a vulnerability scan policy.	write	host *	-
hss:vulnerability:listVulWhiteList	Grants permission to query the vulnerability whitelist.	list	-	g:EnterpriseProjectId
hss:vulnerability:getVulWhiteListDetail	Grants permission to query vulnerability whitelist details.	read	-	g:EnterpriseProjectId
hss:vulnerability:changeVulWhiteList	Grants permission to modify the vulnerability whitelist.	write	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:deleteVulWhiteList	Grants permission to delete an item from the vulnerability whitelist.	write	-	-
hss:vulnerability:addVulWhiteList	Grants permission to add an item to the vulnerability whitelist.	write	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:listVulWhiteListVulOptions	Grants permission to query vulnerability options when adding a whitelist item.	list	-	-
hss:vulnerability:listVulScanTask	Grants permission to query the vulnerability scan task list.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:listVulScanTaskHost	Grants permission to query the list of servers corresponding to a vulnerability scan task.	list	-	g:EnterpriseProjectId
hss:vulnerability:rescanVulScanTask	Grants permission to rescan servers in a vulnerability scan task.	write	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:getVulScanTaskStatistics	Grants permission to query vulnerability scan task statistics.	read	-	g:EnterpriseProjectId
hss:vulnerability:listHostVulStatistics	Grants permission to query vulnerability management statistics.	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHostApps	Grants permission to query details about the software list of servers affected by vulnerabilities.	list	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:listVulHostProcess	Grants permission to query details about the process list of servers affected by vulnerabilities.	list	host *	-
			-	g:EnterpriseProjectId
hss:vulnerability:listVulHandleHistory	Grants permission to query historical vulnerability handling records.	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHostHosts	Grants permission to query the list of servers with vulnerabilities.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:listVulHostVuls	Grants permission to query emergency fixes and unfixed vulnerabilities.	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHostHandle-Vuls	Grants permission to query vulnerabilities handled today and the total vulnerabilities handled.	list	-	g:EnterpriseProjectId
hss:image:listImageNonCompliantApp	Grants permission to query the non-compliant software information of an image.	list	-	g:EnterpriseProjectId
hss:image:batchExportSWRVulList	Grants permission to export vulnerabilities from an SWR image repository in batches.	write	-	g:EnterpriseProjectId
hss:image:batchExportLocalVulList	Grants permission to export local image vulnerabilities in batches.	write	-	g:EnterpriseProjectId
hss:image:getExtendedWeakPassword	Grants permission to query the user-defined weak passwords of an image.	list	-	g:EnterpriseProjectId
hss:image:changeExtendedWeakPassword	Grants permission to modify the user-defined weak passwords of an image.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:listImageBasicImage	Grants permission to query basic image information.	list	-	g:EnterpriseProjectId
hss:image:listImagePwdComplexity	Grants permission to query the password complexity check report of an image.	list	-	g:EnterpriseProjectId
hss:image:listImageWeakPwdUsers	Grants permission to query the image weak password check results of an image.	list	-	g:EnterpriseProjectId
hss:image:listImageRiskConfigs	Grants permission to query the security configuration check results of an image.	list	-	g:EnterpriseProjectId
hss:image:listImageRiskConfigCheck-Rules	Grants permission to query the check items of a specified image security configuration item.	list	-	g:EnterpriseProjectId
hss:image:getImageRiskConfigDetail	Grants permission to query the check results of a specified image security configuration item.	read	-	g:EnterpriseProjectId
hss:image:getImageCheckRuleDetail	Grants permission to query the check reports of an image configuration check item.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:getImageBaselineStatistic	Grants permission to query baseline check statistics, including weak passwords, password complexity, and configuration detection.	read	-	g:EnterpriseProjectId
hss:event:addSystemUserWhiteList	Grants permission to add users to the system user whitelist.	write	-	g:EnterpriseProjectId
hss:event:updateSystemUserWhiteList	Grants permission to modify the system user whitelist.	write	-	g:EnterpriseProjectId
hss:event:listSystemUserWhiteList	Grants permission to query the system user whitelist.	list	-	g:EnterpriseProjectId
hss:event:removeSystemUserWhiteList	Grants permission to remove users from the system user whitelist.	write	-	g:EnterpriseProjectId
hss:container:saveClusters	Grants permission to synchronize cluster information.	write	-	g:EnterpriseProjectId
hss:container:listClusterInfo	Grants permission to query the Kubernetes cluster list.	list	-	g:EnterpriseProjectId
hss:container:listPodInfo	Grants permission to query the basic pod information list.	list	-	g:EnterpriseProjectId
hss:container:showPodDetail	Grants permission to query pod details.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:container:listContainerInfo	Grants permission to query the basic container information list.	list	-	g:EnterpriseProjectId
hss:container:showContainerDetail	Grants permission to query container details.	list	-	g:EnterpriseProjectId
hss:container:listServiceInfo	Grants permission to query the Kubernetes service list.	list	-	g:EnterpriseProjectId
hss:container:showServiceDetail	Grants permission to query Kubernetes service details.	read	-	g:EnterpriseProjectId
hss:container:listEndpointInfo	Grants permission to query the Kubernetes endpoint list.	list	-	g:EnterpriseProjectId
hss:container:showEndpointDetail	Grants permission to query Kubernetes endpoint details.	read	-	g:EnterpriseProjectId
hss:container:listDeployments	Grants permission to query the Kubernetes Deployment list.	list	-	g:EnterpriseProjectId
hss:container:listStatefulSets	Grants permission to query the Kubernetes StatefulSet list.	list	-	g:EnterpriseProjectId
hss:container:listDaemonSets	Grants permission to query the Kubernetes daemon list.	list	-	g:EnterpriseProjectId
hss:container:listJobs	Grants permission to query the Kubernetes common job list.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:container:listCronJobs	Grants permission to query the Kubernetes scheduled task list.	list	-	g:EnterpriseProjectId
hss:vulnerability:showVulAffectedStatics	Grants permission to count the servers affected by vulnerabilities.	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHandleTask	Grants permission to query the vulnerability handling task list.	list	-	g:EnterpriseProjectId
hss:vulnerability:listVulHandleTask-Detail	Grants permission to query vulnerability handling task details.	list	-	g:EnterpriseProjectId
hss:container:isolateK8sContainer	Grants permission to modify the running status of the container.	write	-	g:EnterpriseProjectId
hss:container:getNetworkStatistics	Grants permission to query the container firewall statistics status.	list	-	g:EnterpriseProjectId
hss:container:getClusters	Grants permission to query the cluster list.	list	-	g:EnterpriseProjectId
hss:container:getClusterNetworkInfo	Grants permission to query cluster network information.	read	-	g:EnterpriseProjectId
hss:container:getClusterPolicyList	Grants permission to query the container network policy list.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:container:deletePolicy	Grants permission to delete container network policies.	write	-	g:EnterpriseProjectId
hss:container:createPolicy	Grants permission to create container network policies.	write	-	g:EnterpriseProjectId
hss:container:updatePolicy	Grants permission to update container network policies.	write	-	g:EnterpriseProjectId
hss:container:syncClusterPolicyList	Grants permission to synchronize container network policies.	read	-	g:EnterpriseProjectId
hss:container:syncClusterList	Grants permission to synchronize cluster namespace information.	read	-	g:EnterpriseProjectId
hss:container:getNamespaceList	Grants permission to query the cluster namespace list.	list	-	g:EnterpriseProjectId
hss:container:getNodeList	Grants permission to query the cluster node list.	list	-	g:EnterpriseProjectId
hss:container:syncClusterNodeList	Grants permission to synchronize cluster nodes.	read	-	g:EnterpriseProjectId
hss:vulnerability:getVulScanTaskEstimatedTime	Grants permission to query the estimated time of a vulnerability scan.	read	-	g:EnterpriseProjectId
hss:antiransomware:addRansomwareProtectionPolicy	Grants permission to add ransomware protection policies.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:antiransomware:associateBackupPolicy	Grants permission to apply backup policies to vaults.	write	-	g:EnterpriseProjectId
hss:antiransomware:listBackupPolicy	Grants permission to query the backup policy list.	list	-	g:EnterpriseProjectId
hss:antiransomware:associateProtectionPolicy	Grants permission to switch ransomware protection policies.	write	-	g:EnterpriseProjectId
hss:antiransomware:batchStartProtection	Grants permission to enable ransomware protection.	write	-	g:EnterpriseProjectId
hss:event:getEventAttCk	Grants permission to query the list of ATT&CK attack phase statistics.	list	event *	-
			-	g:EnterpriseProjectId
hss:event:downloadEventSourceFile	Grants permission to download alarm source files.	list	event *	-
			-	g:EnterpriseProjectId
hss:overview:showSecurityScore	Grants permission to query security scores.	list	-	g:EnterpriseProjectId
hss:overview:listSecurityRisk	Grants permission to query the security risk list.	list	-	g:EnterpriseProjectId
hss:overview:showQuotaHostStatistics	Grants permission to query server quota statistics.	list	-	g:EnterpriseProjectId
hss:overview:showAgentStatistics	Grants permission to query the number of agents to be upgraded, online, and offline.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:overview:showHotInformation	Grants permission to query hot news.	list	-	g:EnterpriseProjectId
hss:overview:showSecurityRisk	Grants permission to query security risk information.	list	-	g:EnterpriseProjectId
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	-	g:EnterpriseProjectId
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	-	g:EnterpriseProjectId
hss:event:listEventHandleHistory	Grants permission to query the list of historical events handling.	list	event *	-
			-	g:EnterpriseProjectId
hss:image:listSwrImageRepository	Grants permission to query the image list in the SWR image repository.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:batchScanSwrImage	Grants permission to scan images in the image repository in batches.	write	-	g:EnterpriseProjectId
hss:image:vulnerabilities	Grants permission to query image vulnerability details.	list	-	g:EnterpriseProjectId
hss:image:listVulnerabilityCve	Grants permission to query CVE details about a vulnerability.	list	-	g:EnterpriseProjectId
hss:image:listImageRiskConfigRules	Grants permission to query the check items of a specified image security configuration item.	list	-	g:EnterpriseProjectId
hss:image:runImageSynchronize	Grants permission to synchronize the image list from SWR.	write	-	g:EnterpriseProjectId
hss:event:listEventForensic	Grants permission to query event forensics information.	list	event *	-
			-	g:EnterpriseProjectId
hss:event:listSimilarHandledEvents	Grants permission to query similar handled alarms.	list	event *	-
			-	g:EnterpriseProjectId
hss:event:listSameEvent	Grants permission to query the same alarms.	list	event *	-
			-	g:EnterpriseProjectId
hss:container:getPolicies	Grants permission to query the policy list.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:container:getPolicyDetail	Grants permission to query policy details.	list	-	g:EnterpriseProjectId
hss:container:getOverview	Grants permission to query cluster protection overview.	list	-	g:EnterpriseProjectId
hss:container:getProtectEvents	Grants permission to query cluster protection events.	list	-	g:EnterpriseProjectId
hss:container:getProtectClusters	Grants permission to query cluster protection information.	list	-	g:EnterpriseProjectId
hss:container:changeProtectStatus	Grants permission to change the cluster protection status.	write	-	g:EnterpriseProjectId
hss:container:addWhiteImage	Grants permission to add images to the whitelist.	write	-	g:EnterpriseProjectId
hss:container:listDefaultPolicy	Grants permission to query the default policy template.	list	-	g:EnterpriseProjectId
hss:container:listProtectionItem	Grants permission to query the protection scope.	list	-	g:EnterpriseProjectId
hss:vulnerability:getVulBackupStatistics	Grants permission to query backup statistics of the server corresponding to the vulnerability handling.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:ListVulHostVaults	Grants permission to query the list of server vaults corresponding to vulnerability handling.	list	-	g:EnterpriseProjectId
hss:vulnerability:ListVulHostBackups	Grants permission to query the list of backups that can be rolled back.	list	host *	g:EnterpriseProjectId
hss:vulnerability:RestoreVulHostBackup	Grants permission to roll back with backups.	write	-	g:EnterpriseProjectId
hss:event:exportEvent	Grants permission to export event alarms.	write	event *	-
			-	g:EnterpriseProjectId
hss:event:queryExportTask	Grants permission to query the task of exporting event alarms.	read	event *	-
			-	g:EnterpriseProjectId
hss:event:downloadEvent	Grants permission to download event alarms.	read	event *	-
			-	g:EnterpriseProjectId
hss:ars:createAppWhitelistPolicy	Grants permission to create an application process whitelist policy.	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistPolicy	Grants permission to query the list of application process whitelist policies.	list	-	g:EnterpriseProjectId
hss:ars:changeAppWhitelistPolicy	Grants permission to modify an application process whitelist policy.	write	host *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:ars:deleteAppWhitelistPolicy	Grants permission to delete an application process whitelist policy.	write	-	g:EnterpriseProjectId
hss:ars:showAppWhitelistPolicy	Grants permission to query the application process whitelist policy information.	list	-	g:EnterpriseProjectId
hss:ars:switchAppWhitelistPolicy-Host	Grants permission to modify the protection status of an application process whitelist policy.	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:addAppWhitelistPolicyHost	Grant permissions to add servers to an application process whitelist policy.	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistPolicyHost	Grants permission to query the server list for an application process whitelist policy.	list	-	g:EnterpriseProjectId
hss:ars:deleteAppWhitelistPolicy-Host	Grants permission to remove servers from an application process whitelist policy.	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistHostStatus	Grants permission to query the list of available servers for an application process whitelist policy.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:ars:listAppWhitelistPolicyProcess	Grants permission to query the list of processes that an application process whitelist policy applies to.	list	-	g:EnterpriseProjectId
hss:ars:changeAppWhitelistPolicy-ProcessStatus	Grants permission to modify the process trust status of an application process whitelist policy.	write	-	g:EnterpriseProjectId
hss:ars:addAppWhitelistPolicyProcess	Grants permission to add processes to an application process whitelist policy.	write	host *	-
			-	g:EnterpriseProjectId
hss:ars:listAppWhitelistPolicyProcess-sExtend	Grants permission to query the extended process list for an application process whitelist policy.	list	host *	-
			-	g:EnterpriseProjectId
hss:ars:exportAppWhitelistPolicy-Process	Grants permission to export the list of processes that an application process whitelist policy applies to.	list	host *	-
			-	g:EnterpriseProjectId
hss:ars:switchAppWhitelistPolicy-LearnStatus	Grants permission to modify the learning status of an application process whitelist policy.	write	host *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
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	-	g:EnterpriseProjectId
hss:ars:listAppWhitelistEvent	Grants permission to query the list of suspicious process events detected by application process control.	list	-	g:EnterpriseProjectId
hss:container:deleteSelfBuildK8sClusterDaemonsetInfo	Grants permission to delete a daemonset of the self-built cluster.	write	-	g:EnterpriseProjectId
hss:container:saveSelfBuildK8sClusterDaemonsetInfo	Grants permission to save a daemonset of the self-built cluster.	write	-	g:EnterpriseProjectId
hss:container:showSelfBuildK8sClusterDaemonsetInfo	Grants permission to query a daemonset of the self-built cluster.	read	-	g:EnterpriseProjectId
hss:container:listSelfBuildK8sClusterInfo	Grants permission to query the self-built Kubernetes cluster list.	list	-	g:EnterpriseProjectId
hss:container:createDaemonset	Grants permission to create a daemonset of CCE cluster.	write	-	g:EnterpriseProjectId
hss:vulnerability:listVulRepairCmds	Grants permission to query vulnerability fixing commands.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:listUrgentVulnera-bilities	Grants permission to query the emergency vulnerability list.	list	-	g:EnterpriseProjectId
hss:antivirus:createAntivirusTask	Grants permission to create virus scan tasks.	write	host *	-
			-	g:EnterpriseProjectId
hss:antivirus:listAntivirusTask	Grants permission to query the virus scan task list.	list	-	g:EnterpriseProjectId
hss:antivirus:switchAntivirusTask	Grants permission to cancel virus scan tasks.	write	host *	-
			-	g:EnterpriseProjectId
hss:antivirus:listAntivirusHost	Grants permission to query the list of servers available for virus scan.	list	-	g:EnterpriseProjectId
hss:antivirus:createAntivirusPolicy	Grants permission to create custom virus scan policies.	write	host *	-
			-	g:EnterpriseProjectId
hss:antivirus:listAntivirusPolicy	Grants permission to query the list of custom virus scan policies.	list	-	g:EnterpriseProjectId
hss:antivirus:listAntivirusResult	Grants permission to query the list of virus scan results.	list	-	g:EnterpriseProjectId
hss:antivirus:operateAntivirusResult	Grants permission to handle virus scan results.	write	-	g:EnterpriseProjectId
hss:antivirus:exportAntivirusResult	Grants permission to export virus scan results.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:antivirus:showAntivirusStatistic	Grants permission to query virus scan statistics.	list	-	g:EnterpriseProjectId
hss:image:showImageFullScanProgress	Grants permission to query the progress of a full image scan.	list	-	g:EnterpriseProjectId
hss:host:changeHostIgnoreStatus	Grants permission to ignore or unignore servers.	write	host *	-
			-	g:EnterpriseProjectId
hss:host:listIgnoreHosts	Grants permission to query ignored servers.	list	host *	-
			-	g:EnterpriseProjectId
hss:image:batchExportBaselineTask	Grants permission to export image baseline check results.	write	-	g:EnterpriseProjectId
hss:image:showImageSecurityReportStatistic	Grants permission to query the number of image scan results to be exported.	write	-	g:EnterpriseProjectId
hss:vulnerability:exportVuls	Grants permission to create vulnerability export tasks.	write	-	g:EnterpriseProjectId
hss:exportTask:queryExportTask	Grants permission to query export tasks.	list	-	g:EnterpriseProjectId
hss:file:downloadExportedFile	Grants permission to download files.	list	-	g:EnterpriseProjectId
hss:image:listGlobalVulnerabilities	Grants permission to query vulnerability details about a tenant image.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:image:listVulnerabilityImages	Grants permission to query details about images in the image repository affected by a vulnerability.	list	-	g:EnterpriseProjectId
hss:setting:getPluginInstallScript	Grants permission to query server plug-in information.	list	-	g:EnterpriseProjectId
hss:setting:getPluginList	Grants permission to query the plug-in installation guide.	list	-	g:EnterpriseProjectId
hss:setting:getAutoOpenQuotaStatus	Grants permission to query the status of automatic quota binding.	read	-	g:EnterpriseProjectId
hss:setting:changeAutoOpenQuotaStatus	Grants permission to modify the status of automatic quota binding.	write	-	g:EnterpriseProjectId
hss:image:batchExportSWRVulTask	Grants permission to export SWR image vulnerability scan results.	write	-	g:EnterpriseProjectId
hss:image:batchExportLocalVulTask	Grants permission to export local image vulnerability scan results.	write	-	g:EnterpriseProjectId
hss:vulnerability:exportVulReport	Grants permission to export vulnerability reports in HTML format.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
hss:vulnerability:getVulReportData	Grants permission to obtain vulnerability reports in PDF format.	list	-	g:EnterpriseProjectId
hss:setting:getAgentAutoUpgradeStatus	Grants permission to query the status of automatic agent upgrade.	read	-	g:EnterpriseProjectId
hss:setting:changeAgentAutoUpgradeStatus	Grants permission to modify the status of automatic agent upgrade.	write	-	g:EnterpriseProjectId
hss:quota:showProductdataOfferingInfos	Grants permission to query product information.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageAppInfo	Grants permission to query the local software image list.	list	-	g:EnterpriseProjectId
hss:image:listLocalImageAppVulnerabilities	Grants permission to query the vulnerability list of a piece of software in a local image.	list	-	g:EnterpriseProjectId

Each API of HSS usually supports one or more actions. **Table 5-147** lists the supported actions and dependencies.

Table 5-147 Actions and dependencies supported by HSS APIs

API	Action	Dependencies
POST /v5/{project_id}/host-management/groups	hss:host:addHostsGroup	eps:enterpriseProjects:list

API	Action	Dependencies
PUT /v5/{project_id}/event/blocked-ip	hss:event:changeBlockedIp	eps:enterpriseProjects:list
GET /v5/{project_id}/backup/policy	hss:antiransomware:getRansomwareHSSBackupPolicyInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/container/nodes	hss:container:listContainerNodes	eps:enterpriseProjects:list
GET /v5/{project_id}/host-management/groups	hss:host:listHostGroups	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}/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}/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}/webtamper/hosts	hss:wtp:listWtpProtectHost	• eps:enterpriseProjects:list • vpc:ports:list

API	Action	Dependencies
POST /v5/{project_id}/webtamper/static/status	hss:wtp:setWtpProtectionStatusInfo	eps:enterpriseProjects:list
POST /v5/{project_id}/webtamper/rasp/status	hss:wtp:setWtpProtectSwitch	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/protection/open	hss:antiransomware:startRansomwareProtection	eps:enterpriseProjects:list
POST /v5/{project_id}/ransomware/protection/close	hss:antiransomware:stopRansomwareProtection	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
GET /v5/{project_id}/asset/statistics	hss:asset:getAssetStatistic	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-launchs	hss:asset:listAutoLaunchs	eps:enterpriseProjects:list

API	Action	Dependencies
GET /v5/{project_id}/asset/auto-launch/statistics	hss:asset:listAutoLaunchStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/midwares/detail	hss:asset:listJarPackageHostInfo	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/midwares	hss:asset:listJarPackageStatistics	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/process/statistics	hss:asset:listProcessStatistics	eps:enterpriseProjects:list
GET /v5/{project_id}/asset/user/change-history	hss:asset:listUserChangeHistories	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}/baseline/check-rule/detail	hss:baseline:getCheckRuleDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/risk-config/{check_name}/detail	hss:baseline:getRiskConfigDetail	eps:enterpriseProjects:list
GET /v5/{project_id}/baseline/password-complexity	hss:baseline:listPasswordComplexity	eps:enterpriseProjects:list

API	Action	Dependencies
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/weak-password-users	hss:baseline:listWeakPasswordUsers	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/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/isolated-file	hss:event:listIsolatedFile	eps:enterpriseProjects:list
GET /v5/{project_id}/event/events	hss:event:listSecurityEvents	eps:enterpriseProjects:list
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

API	Action	Dependencies
GET /v5/{project_id}/host-management/hosts	hss:host:listHostStatus	• eps:enterpriseProjects:list • vpc:ports:list • eip:publicIps:list
POST /v5/{project_id}/host-management/protection	hss:host:switchHostsProtectStatus	eps:enterpriseProjects:list
POST /v5/{project_id}/policy/deploy	hss:policy:associatePolicyGroup	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/{key}	hss:quota:deleteResourceInstanceTag	eps:enterpriseProjects:list
GET /v5/{project_id}/billing/quotas	hss:quota:getResourceQuotas	eps:enterpriseProjects:list
GET /v5/{project_id}/billing/quotas-detail	hss:quota:listQuotasDetail	eps:enterpriseProjects:list
PUT /v5/{project_id}/vulnerability/status	hss:vulnerability:changeVulStatus	eps:enterpriseProjects:list
GET /v5/{project_id}/vulnerability/host/{host_id}	hss:vulnerability:listHostVuls	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

API	Action	Dependencies
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/scan-tasks	hss:vulnerability:listVulScanTask	-
GET /v5/{project_id}/vulnerability/scan-task/{task_id}/hosts	hss:vulnerability:listVulScanTaskHost	-
GET /v5/{project_id}/vulnerability/statistics	hss:vulnerability:listHostVulStatistics	-
GET /v5/{project_id}/image/baseline/risk-configs	hss:image:listImageRiskConfigs	-
GET /v5/{project_id}/image/baseline/check-rule/detail	hss:image:getImageCheckRuleDetail	-
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	-

API	Action	Dependencies
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}/product/productdata/offering-infos	hss:quota:showProductdataOfferingInfos	-

Resource

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-148**, 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 HSS.

Table 5-148 Resource types supported by HSS

Resource Type	URN
host	hss:<region>:<account-id>:host:<host-id>
event	hss:<region>:<account-id>:event:<event-id>
baseline	hss:<region>:<account-id>:baseline:<type>/<check_rule_id>
policy	hss:<region>:<account-id>:policy:<resource-type>/<type-id>

Conditions

HSS does not support service-specific condition keys in SCP statements.

HSS can use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.8.4 SecMaster

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 permission 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 resource 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 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 resource types 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 following table lists the actions that you can define in SCP statements for SecMaster.

Table 5-149 Actions supported by SecMaster

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 the playbook version.	write	playbook *	-
secmaster:playbook:approve	Grants the permission to review a playbook.	write	playbook *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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:createVersionRule	Grants the permission to create a rule for a playbook version.	write	playbook *	-
secmaster:playbook:createVersionAction	Grants the permission to create an action for a playbook version.	write	playbook *	-
secmaster:playbook:getVersion	Grants the permission to obtain a playbook version.	read	playbook *	-
secmaster:playbook:getVersionRule	Grants the permission to obtain rules for a playbook version.	read	playbook *	-
secmaster:playbook:deleteVersion	Grants the permission to delete a playbook version.	write	playbook *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
secmaster:playbook:deleteVersionRule	Grants the permission to delete a rule for a playbook version.	write	playbook *	-
secmaster:playbook:deleteVersionAction	Grants the permission to delete an action for a playbook version.	write	playbook *	-
secmaster:playbook:updateVersion	Grants the permission to update a playbook version.	write	playbook *	-
secmaster:playbook:updateVersionRule	Grants the permission to update a rule for a playbook version.	write	playbook *	-
secmaster:playbook:updateVersionAction	Grants the permission to update an action for a playbook version.	write	playbook *	-
secmaster:playbook:listVersions	Grants the permission to obtain the list of playbook versions.	list	playbook *	-
secmaster:playbook:listVersionActions	Grants the permission to obtain the list of actions for a playbook version.	list	playbook *	-
secmaster:playbook:getInstance	Grants the permission to query details about a playbook instance.	read	playbook *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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:list	Grants the permission to query the workspace list.	list	workspace *	-
secmaster:workspace:create	Grants the permission to create a workspace.	write	workspace *	-
secmaster:workspace:update	Grants the permission to update a workspace.	write	workspace *	-
secmaster:workspace:get	Grants the permission to obtain workspace details.	read	workspace *	-
secmaster:workspace:delete	Grants the permission to delete a workspace.	write	workspace *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
secmaster:task:list	Grants the permission to query the to-do list.	list	task *	-
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
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
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 *	-
secmaster:incident:delete	Grants the permission to delete an incident.	write	incident *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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:updateFiled	Grants the permission to update a layout field.	write	layout *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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 *	-
secmaster:table:updateSchema	Grants the permission to design a table.	write	table *	-

Each API of SecMaster usually supports one or more actions. **Table 5-150** lists the supported actions and dependencies.

Table 5-150 Actions and dependencies supported by SecMaster APIs

API	Action	Dependencies
GET /v1/{project_id}/workspaces/{workspace_id}/soc/playbooks/{playbook_id}	secmaster:playbook:get	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/workflows/{workflow_id}	secmaster:workflow:delete	-
GET /v1/{project_id}/workspacesPOST /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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/incidents/types/layout	secmaster:incident:bindLayout	-

API	Action	Dependencies
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	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/vulnerabilities/types/enable	secmaster:vulnerability:enableType	-
DELETE /v1/{project_id}/subscriptions/orders	secmaster:subscription:deletePostPaidOrder	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules	secmaster:alertRule:delete	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/enable	secmaster:alertRule:enable	-

API	Action	Dependencies
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/disable	secmaster:alertRule:disable	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/metrics	secmaster:alertRule:listMetrics	-
POST /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/simulation	secmaster:alertRule:createSimulation	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates	secmaster:alertRuleTemplate:list	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/{template_id}	secmaster:alertRuleTemplate:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/siem/alert-rules/templates/metrics	secmaster:alertRuleTemplate:listMetrics	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses	secmaster:dataclass:create	-
PUT /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:update	-
DELETE /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:delete	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}	secmaster:dataclass:get	-
GET /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses	secmaster:dataclass:list	-
POST /v1/{project_id}/workspaces/{workspace_id}/soc/dataclasses/{dataclass_id}/fields	secmaster:dataclass:createField	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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:updateFiled	-
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	-
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	-

API	Action	Dependencies
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 in **Table 5-151**, 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 5-151 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>
alertRuleTemplate	secmaster:<region>:<account-id>:alertRuleTemplate:<workspace-id>/<alertRuleTemplate-id>

Resource Type	URN
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>

Conditions

SecMaster does not support service-specific condition keys in SCP statements. SecMaster can use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.8.5 Cloud Firewall (CFW)

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.

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 edit a custom SCP policy, 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 an SCP 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 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 CFW, see **Conditions**.

The following table lists the actions that you can define in SCP statements for CFW

Table 5-152 Actions supported by CFW

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:acl:createAclRule	Grants permission to create an acl rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:deleteAclRule	Grants permission to delete an acl rule.	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:deleteHitCount	Grants permission to delete acl rule hit count.	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:listDomainParseServers	Grants permission to get domain parse server.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getDomainParseResult	Grants permission to parse domain.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:getExportStatus	Grants permission to get acl export status.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:getImportStatus	Grants permission to get acl import status.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:getImportTemplate	Grants permission to get acl import template.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:listAclRules	Grants permission to list acl rules.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:listAclTags	Grants permission to list acl rule tags.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:updateAclRule	Grants permission to update acl rule.	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:updateAclRuleAction	Grants permission to update acl rule action.	write	acl *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateDomainParseServer	Grants permission to update domain parse server.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:acl:setPriority	Grants permission to set acl rule priority.	write	acl *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:create	Grants permission to create blackwhite list.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:delete	Grants permission to delete blackwhite list.	write	blackWhiteList *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:list	Grants permission to list blackwhite lists.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:blackWhiteList:update	Grants permission to update blackwhite list.	write	blackWhiteList *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:domainGroup:update	Grants permission to update domainGroup.	write	domainGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:domainGroup:create	Grants permission to create domainGroup.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:domainGroup:delete	Grants permission to delete domainGroup.	write	domainGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:domainGroup:list	Grants permission to list domainGroup.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:eip:count	Grants permission to get eip statistics.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:eip:list	Grants permission to list eip.	list	instance *	g:ResourceTag/<tag-key>
cfw:eip:updateProtectStatus	Grants permission to change eip protect status.	write	eip *	-
			-	g:EnterpriseProjectId
cfw:instance:checkNameRepeat	Grants permission to check if cfw name repeat.	read	-	-
cfw:instance:listAdvanceIpsRules	Grants permission to list cfw advance ips rules.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:listUsedEr	Grants permission to list used er.	list	-	-
cfw:instance:listUsedInspectionVpc	Grants permission to list used vpc.	list	-	-
cfw:instance:addLogConfig	Grants permission to add CFW log config.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	cfw:LogGroupId
cfw:instance:updateCustomRule	Grants permission to update CFW custom ips rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateCustomRuleAction	Grants permission to update CFW custom ips rule action.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateLogConfig	Grants permission to update CFW LTS log config.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	cfw:LogGroupId
cfw:instance:createInstance	Grants permission to create an CFW instance.	write	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
cfw:instance:deletePostPaidInstance	Grants permission to delete post paid CFW instance.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:createCaptureTask	Grants permission to create CFW capture task.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createCustomRule	Grants permission to create CFW custom rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createTags	Grants permission to create CFW tags.	tagging	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
cfw:instance:deleteInstance	Grants permission to delete CFW instance.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteCaptureTask	Grants permission to delete CFW capture task.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteCustomRule	Grants permission to delete CFW custom ips rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteLogSearchHistory	Grants permission to delete CFW log search history.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteTags	Grants permission to delete CFW tags.	tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:exportLog	Grants permission to export log.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listInstanceByTags	Grants permission to list cfw by tags.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	g:TagKeys
cfw:instance:getBaseVersion	Grants permission to get cfw base version.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getCaptureTaskResult	Grants permission to get cfw capture task result.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getCustomRule	Grants permission to get cfw custom rule.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getDomainParseServerStatus	Grants permission to get cfw domain parse server status.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getIpsMode	Grants permission to get cfw ips mode.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getIpsStatus	Grants permission to get cfw ips status.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getLogConfig	Grants permission to get cfw log config.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:getMaxCapturePacket-Num	Grants permission to get cfw user max capture packet number.	read	-	-
cfw:instance:getPolicyStatistics	Grants permission to get cfw policy statistics.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listProjectTags	Grants permission to list project tags.	list	-	-
cfw:instance:getRegionDb	Grants permission to get cfw region db.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listInstanceTags	Grants permission to list cfw tags.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listInstance	Grants permission to list CFW instances.	list	instance *	-
cfw:instance:getInstance	Grants permission to get CFW instances detail.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listAccessControlLog	Grants permission to list CFW access control log.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listAttackLog	Grants permission to list CFW attack log.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listCaptureTask	Grants permission to list CFW capture tasks.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:listCustomRule	Grants permission to list CFW custom ips rule.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getEw	Grants permission to get cfw east-west firewall.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listFlowLog	Grants permission to list cfw flow log.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listIpsRule	Grants permission to list cfw ips rules.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listProtectedVpc	Grants permission to list cfw protect vpcs.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateIpsMode	Grants permission to update cfw ips mode.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateAdvanceIpsRule	Grants permission to update cfw advance ips rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateIpsRuleAction	Grants permission to update cfw ips rule mode.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateIpsStatus	Grants permission to update cfw ips status.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:updateEwProtectedStatus	Grants permission to update cfw east-west firewall protect status.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:saveTags	Grants permission to save cfw tags.	tagging	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
cfw:instance:startBaseVersion	Grants permission to start cfw base version.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:stopBaseVersion	Grants permission to stop cfw base version.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:stopCaptureTask	Grants permission to stop cfw capture task.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateAlarmConfig	Grants permission to update cfw alarm config.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAlarmConfig	Grants permission to get cfw alarm config.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:upgradeInstance	Grants permission to upgrade cfw.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:updateName	Grants permission to update cfw name.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAccessControlLogStatistics	Grants permission to get cfw access control log statistics.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAttackLogStatistics	Grants permission to get cfw attack log statistics.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getLogSearchHistory	Grants permission to get cfw log search history.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getEngineLogStatistics	Grants permission to get cfw engine log statistics.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getFlowLogStatistics	Grants permission to get cfw flow log statistics.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getIpLogStatistics	Grants permission to get cfw ip log statistics.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:updateIpGroupMember	Grants permission to update cfw ip group member.	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:ipGroup:createIpGroup	Grants permission to change cfw ip group member.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:createIpGroupMember	Grants permission to create cfw ip group member.	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:deleteIpGroup	Grants permission to delete cfw ip group.	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:deleteIpGroupMember	Grants permission to delete cfw ip group member.	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:getIpGroup	Grants permission to get cfw ip group.	read	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:listIpGroups	Grants permission to list cfw ip groups.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:listIpGroupMember	Grants permission to list cfw ip group members.	list	ipGroup *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:ipGroup:updateIpGroup	Grants permission to update cfw ip group.	write	ipGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:updateServiceGroupMember	Grants permission to update cfw service group member.	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:create	Grants permission to create cfw service group member.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:createServiceGroupMember	Grants permission to create cfw service group member.	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:delete	Grants permission to delete cfw service group.	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:deleteServiceGroupMember	Grants permission to delete cfw service group member.	write	serviceGroup *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:get	Grants permission to get cfw service group.	read	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:list	Grants permission to list cfw service groups.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:listServiceGroup-Member	Grants permission to list cfw service group members.	list	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:serviceGroup:update	Grants permission to update cfw service group.	write	serviceGroup *	-
			instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:enableMultiAccount	Grants permission to enable multi account.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listAccounts	Grants permission to list accounts.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:listOrganizationTree	Grants permission to list organization tree.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:addAccount	Grants permission to add account.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteAccount	Grants permission to delete account.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getProtectedVpc	Grants permission to get protected vpc.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteProtectedVpc	Grants permission to delete protected vpc.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:addProtectedVpc	Grants permission to add protected vpc.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateProtectedVpc	Grants permission to update protected vpc.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateAntiVirusStatus	Grants permission to update cfw anti virus status.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAntiVirusStatus	Grants permission to get cfw anti virus status.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cfw:instance:updateAntiVirusRule	Grants permission to update cfw anti virus rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getAntiVirusRule	Grants permission to get cfw anti virus rule.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:listReportProfile	Grants permission to list cfw report profile rules.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:createReportProfile	Grants permission to create cfw report profile rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:updateReportProfile	Grants permission to update cfw report profile rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:getReportProfile	Grants permission to show cfw report profile rule.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cfw:instance:deleteReportProfile	Grants permission to delete cfw report profile rule.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Each API of CFW usually supports one or more actions. **Table 5-153** lists the supported actions and dependencies.

Table 5-153 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	-
POST /v1/{project_id}/firewall/east-west	cfw:instance:createInstance	• er:instances:list • er:instances:listVpcAttachments • er:attachments:create • vpc:vpcs:list • vpc:subnets:get • vpc:subnets:create • vpc:routeTables:list • vpc:routeTables:update • vpc:quotas:list • nat:natGateways:list
DELETE /v2/{project_id}/firewall/{resource_id}	cfw:instance:deleteInstance	-
GET /v1/{project_id}/firewall/east-west	cfw:instance:getEw	• er:instances:listVpcAttachments • vpc:vpcs:list • nat:natGateways:list • er:instances:listVpcAttachments • er:instances:get
POST /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/create	cfw:instance:createTags	-

API	Action	Dependencies
DELETE /v2/{project_id}/cfw-cfw/{fw_instance_id}/tags/delete	cfw:instance:deleteTags	-
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	-
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	-
DELETE /v1/{project_id}/address-items	cfw:ipGroup:deleteIpGroupMember	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
DELETE /v1/{project_id}/address-sets/{set_id}	cfw:ipGroup:deleteIpGroup	-
POST /v1/{project_id}/firewall/east-west/protect	cfw:instance:updateEwProtectedStatus	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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/{set_id}	cfw:domainGroup:list	-
POST /v1/{project_id}/acl-rule	cfw:acl:createAclRule	-
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 SCP applies to. If you specify a resource type for any action in **Table 5-154**, 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 CFW.

Table 5-154 Resource types supported by CFW

Resource Type	URN
blackWhiteList	cfw:<region>:<account-id>:blackWhiteList:<blackWhiteList-id>
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

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, cfw) apply only to operations of the xx service. For details, see **Table 5-155**.
  - 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 SCP 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 SCP for CFW. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-155 Service-specific condition keys supported by CFW

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
cfw:LogGroupId	string	Single-valued	Filters access based on the LTS log group ID in the request.

5.10.8.6 Data Security Center (DSC)

The Service Control Policies (SCPs) in the Organizations service can use these authorization elements to set access control policies.

SCPs do not actually grant any permissions to a principal. They only set the permission 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 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 SCP 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 resource types defined by DSC, see **Resources**.
- The **Condition Key** column includes keys that you can specify in the Condition element of an SCP 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 condition keys defined by DSC, see **Conditions**.

The following table lists the actions that you can define in SCP statements for DSC.

Table 5-156 Actions supported by DCS

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dsc:asset:delete	Grants permission to delete data assets.	write	asset *	-
dsc:asset:list	Grants permission to query the data asset list.	list	asset *	-
dsc:asset:create	Grants permission to add data assets.	write	asset *	-
dsc:asset:update	Grants permission to update data asset information.	write	asset *	-
dsc:maskTask:operate	Grants permission to perform operations on masking tasks (such as starting, stopping, enabling, and disabling masking tasks).	write	maskTask *	-
dsc:maskTask:listSubTasks	Grants permission to query the subtask list of a masking task.	list	maskTask *	-
dsc:common:operate	Grants permission to operate DSC generic resources.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dsc:common:list	Grants permission to query the DSC generic resource list.	list	-	-
dsc:scanTask:create	Grants permission to create sensitive data scanning tasks.	write	scanTask *	-
dsc:scanTask:list	Grants permission to query the list of sensitive data scanning tasks or subtasks.	list	scanTask *	-
dsc:scanTask:getResults	Grants permission to query the scan result of a single scan job.	read	scanTask *	-
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	-	-
dsc:scanRuleGroup:delete	Grants permission to delete scan rule groups.	write	-	-
dsc:scanRule:list	Grants permission to query the scan rule list.	list	scanRule *	-
dsc:scanRule:create	Grants permission to create scan rules.	write	scanRule *	-
dsc:scanRule:update	Grants permission to update scan rules.	write	scanRule *	-
dsc:scanRule:delete	Grants permission to delete scan rules.	write	scanRule *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
dsc:watermark:embed	Grants permission to embed watermarks into documents, images, or databases.	write	-	-
dsc:watermark:extract	Grant permission to extract watermarks from documents, images, or databases.	write	-	-

A DSC API usually corresponds to one or more actions. **Table 5-157** lists the supported actions and dependencies.

Table 5-157 Actions and dependencies supported by DSC APIs

API	Action	Dependency
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

API	Action	Dependency
GET/v1/{project_id}/period/product/specification	dsc:common:list	-
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	-

API	Action	Dependency
POST/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:create	-
PUT/v1/{project_id}/sdg/server/scan/rules	dsc:scanRule:update	-
DELETE/v1/{project_id}/sdg/server/scan/rules/{rule_id}	dsc:scanRule:delete	-
GET/v1/{project_id}/sdg/scan/job/{job_id}/results	dsc:scanTask:getResults	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs/{db_id}/tables	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/dbs/{table_id}/columns	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/obs/buckets	dsc:common:list	-
GET/v1/{project_id}/sdg/server/relation/jobs/{job_id}/obs/{bucket_id}/files	dsc:common:list	-
POST/v1/{project_id}/data/mask	dsc:sensitiveData:mask	-

API	Action	Dependency
POST/v1/{project_id}/doc-address/watermark/embed	dsc:watermark:embed	-
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	-

API	Action	Dependency
POST/v1/{project_id}/sdg/doc/watermark/extract	dsc:watermark:extract	-
GET/v1/{project_id}/sdg/asset/{asset_type}/{asset_id}/detail	dsc:common:list	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-158**, the resource URN must be specified in the SCP 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 SCP policy statements for DSC.

Table 5-158 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 SCP policies.

DSC can use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.8.7 Private Certificate Authority (PCA)

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.

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 for the **Resource** element of your statements.
  - Required resources are marked with asterisks (*) in the table.

  For details about the resource types defined by the PCA, see **Table 5-161**.
- 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 PCA, see **Conditions**.

The following table lists the actions that you can define in SCP statements for PCA.

Table 5-159 Actions supported by PCA

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
pca:ca:create	Grants the permission to create a private CA.	write	ca *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
pca:ca:delete	Grants the permission to delete a private CA.	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
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>
			-	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
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>
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
pca:ca:deleteTag	Grants the permission to delete a private CA tag.	tagging	ca *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • g:TagKeys
pca:ca:listTags	Grants the permission to query the tag list of a private CA.	list	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:ca:listAllTags	Grants the permission to query the private CA tag list.	list	ca *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
pca:ca:listByTag	Grants the permission to query the private CA list by tag.	list	ca *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
pca:ca:issueCert	Grants the permission to issue a private certificate.	write	ca *	-
			-	• g:EnterpriseProjectId • pca:CommonName
pca:ca:issueCertByCsr	Grants the permission to issue private certificates based on CSRs.	write	ca *	-
			-	• g:EnterpriseProjectId • pca:CommonName
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
pca:ca:revokeCert	Grants the permission to revoke a private certificate.	write	ca *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
pca:cert:get	Grants the permission to query private certificate details.	read	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
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	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
pca:cert:deleteTag	Grants the permission to delete a private certificate tag.	tagging	-	• g:EnterpriseProjectId • g:TagKeys
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	-	-
pca:cert:listByTag	Grants the permission to query the private certificate list by tag.	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
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 5-160** lists the actions and dependencies supported by PCA APIs.

Table 5-160 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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
POST /v1/private-certificate-authorities/{ca_id}/crl/enable	pca:ca:enableCrl	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-161**, 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 PCA.

Table 5-161 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 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, 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 5-162**.
  - 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 operators, see Condition operators.

The following table lists the condition keys that you can define in SCPs for PCA. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-162 Service-specific condition keys supported by PCA

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
pca:CommonName	string	Single-valued	Filters access based on the common name of the certificate in the request parameters.

5.10.8.8 SSL Certificate Manager (SCM)

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.

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 for the **Resource** element of your statements.
  - Required resources are marked with asterisks (*) in the table.

For details about the resource types defined by the SCM, see **Table 5-165**.

- 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 SCM, see **Conditions**.

The following table lists the actions that you can define in SCP statements for SCM.

Table 5-163 Actions supported by SCM

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
scm:cert:subscribe	Grants the permission to buy a certificate.	write	cert *	-
			-	g:EnterpriseProjectId
scm:cert:update	Grants the permission to update a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:delete	Grants the permission to delete a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:apply	Grants the permission to request a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • scm:DomainNames • scm:ValidationMethod • scm:KeyAlgorithm

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
scm:cert:revoke	Grants the permission to revoke a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:cancel	Grants the permission to cancel a certificate request.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:reissue	Grants the permission to re-issue a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • scm:DomainNames • scm:ValidationMethod
scm:cert:push	Grants the permission to push a certificate to other service.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:import	Grants the permission to import a certificate.	write	cert *	-
			-	g:EnterpriseProjectId
scm:cert:export	Grants the permission to export a certificate.	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:upload	Grants the permission to upload a certificate to SCM.	write	cert *	-
			-	g:EnterpriseProjectId
scm:cert:download	Grants the permission to download a certificate.	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
scm:cert:save	Grants the permission to supplement certificate information.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:addDomain	Grants the permission to add more domain names for a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • scm:DomainNames
scm:cert:expandQuota	Grants the permission to expand the certificate quota.	write	-	g:EnterpriseProjectId
scm:cert:renew	Grants the permission to renew a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:unsubscribe	Grants the permission to unsubscribe from a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:autoRenew	Grants the permission to enable automatic certificate renewal.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:list	Grants the permission to query the certificate list.	list	cert *	-
			-	g:EnterpriseProjectId
scm:cert:get	Grants the permission to query certificate details.	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
scm:cert:getApplicationInfo	Grants the permission to query certificate supplementation information.	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listPushHistory	Grants the permission to query certificate push records.	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:getDomainValidation	Grants the permission to query domain name verification information.	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:checkDomain	Grants the permission to verify the certificate domain name ownership.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listDeployedResources	Grants the permission to obtain the resources associated with the certificate.	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:deletePrivacyAuthorization	Grants the permission to cancel privacy authorization.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:enableAutoDeploy	Grants the permission to automatically deploy a certificate.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listAutoDeployedResources	Grants the permission to query the list of certificates that are automatically deployed.	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
scm:cert:listCertificatesByTag	Grants the permission to query the certificate list by tag.	list	cert *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
scm:cert:createTag	Grants the permission to create or update a tag.	tagging	cert *	g:ResourceTag/<tag-key>
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
scm:cert:listTagsByCertificate	Grants the permission to query the certificate tag list.	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listAllTags	Grants the permission to query the list of all tags.	list	cert *	-
scm:cert:seekHelp	Grants the permission to send a help-seeking email.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:uploadAuthentication	Grants the permission to upload authentication information.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm::createCsr	Grants the permission to create a CSR.	write	-	-
scm::listCsr	Grants the permission to query the CSR list.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
scm::getCsr	Grants the permission to query CSR details.	read	-	-
scm::getCsrPrivateKey	Grants the permission to obtain the CSR private key.	read	-	-
scm::updateCsr	Grants the permission to update a CSR.	write	-	-
scm::deleteCsr	Grants the permission to delete a CSR.	write	-	-
scm::uploadCsr	Grants the permission to upload a CSR.	write	-	-
scm::createDomainMonitor	Grants the permission to add a domain name to be monitored.	write	-	-
scm::updateDomainMonitor	Grants the permission to update domain names to be monitored.	write	-	-
scm::updateDomainMonitorSwitch	Grants the permission to enable or disable domain name monitoring.	write	-	-
scm::deleteDomainMonitor	Grants the permission to delete a monitored domain name.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
scm::getDomainMonitor	Grants the permission to query details about the domain name to be monitored.	read	-	-
scm::listDomainMonitors	Grants the permission to query the list of domain names to be monitored.	list	-	-
scm:cert:operateNotification	Grants the permission to configure certificate notifications.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm::orderDomainMonitor	Grants the permission to buy the domain name monitoring quota.	write	-	-
scm:cert:deployResources	Grants the permission to deploy the certificate to other service resources.	write	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:listDeployResourcesHistory	Grants permission to query the deployment history of a certificate.	list	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId
scm:cert:getDeployQuota	Grants the permission to obtain the certificate deployment quota.	read	cert *	g:ResourceTag/<tag-key>
			-	g:EnterpriseProjectId

Each API of SCM usually supports one or more actions. **Table 5-164** lists the actions and dependencies supported by SCM APIs.

Table 5-164 Actions and dependencies supported by SCM APIs

API	Action	Dependencies
GET /v3/scm/certificates	scm:cert:list	-
POST /v3/scm/certificates/import	scm:cert:import	-
GET /v3/scm/certificates/{certificate_id}	scm:cert:get	-
POST /v3/scm/certificates/{certificate_id}/export	scm:cert:export	-
POST /v3/scm/certificates/{certificate_id}/push	scm:cert:push	-
DELETE /v3/scm/certificates/{certificate_id}	scm:cert:delete	-
POST /v3/scm/certificates/{certificate_id}/read	scm:cert:getApplicationInfo	-
POST /v3/scm/domain/monitor/subscribe	scm::orderDomainMonitor	-
PUT /v3/scm/domain/monitor/change	scm::orderDomainMonitor	-
POST /v3/scm/certificates/{certificate_id}/deploy	scm:cert:deployResources	-
GET /v3/scm/certificates/{certificate_id}/deploy-history	scm:cert:listDeployResourcesHistory	-
GET /v3/scm/certificates/{certificate_id}/deploy-quota	scm:cert:getDeployQuota	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-165**, 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 SCM.

Table 5-165 Resource types supported by SCM

Resource Type	URN
cert	scm:<region>:<account-id>:cert:<cert-id>

Conditions

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, scm:) apply only to operations of EVS. For details, see **Table 5-166**.
  - 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 operators, see Condition operators.

The following table lists the condition keys that you can define in SCPs for SCM. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-166 Service-specific condition keys supported by SCM

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
scm:DomainNames	string	Multivalued	This API is used to filter access requests based on the domain name in the request.
scm:ValidationMethod	string	Single-valued	This API is used to filter access requests based on the authentication mode in the request.
scm:KeyAlgorithm	string	Single-valued	This API is used to filter access requests based on the key algorithm in the request.

5.10.8.9 Cloud Bastion Host (CBH)

The Organizations 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 IAM custom identity policies and 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 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 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 CBH, see **Resources**.

- The **Condition Key** column includes keys that you can specify in the Condition element of an SCP 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 following table lists the actions that you can define in SCP statements for CBH.

Table 5-167 Actions supported by CBH

Action	Description	Access Level	Resource Type (*: Required)	Condition Key	Alias
cbh::listAvailableZones	Grants the permission to query service AZs.	List	-	-	-
cbh::getEcsQuota	Grants the permission to obtain the ECS quota.	Read	-	-	-
cbh::getQuota	Grants the permission to query the CBH instance quotas.	Read	-	-	-
cbh::listSpecifications	Queries protection specifications.	List	-	-	-
cbh:instance:listInstances	Grants the permission to list instances.	List	instance *	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key	Alias
cbh:instance:getInstanceStatus	Grants the permission to query the CBH status.	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:startInstance	Grants the permission to start a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:stopInstance	Grants the permission to disable a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:rebootInstance	Grants the permission to restart a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:upgradeInstance	Grants the permission to upgrade a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:loginInstance	Grants the permission to log in to a CBH instance as an IAM user.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:resetInstancePassword	Grants the permission to reset a password for logging in to a CBH.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key	Alias
cbh:instance:resetInstanceLoginMethod	Grants the permission to reset the CBH instance login mode.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:deleteInstance	Grants the permission to delete a faulty CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:alterInstance	Grants the permission to change a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:createInstance	Grants the permission to create a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:RequestTag/tag-key • g:TagKeys • cbh:VpcId • cbh:SubnetId • cbh:AllowBindPublicIp	-
cbh:instance:bindInstanceEip	Grants the permission to bind an EIP to a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:unbindInstanceEip	Grants the permission to unbind an EIP from a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key	Alias
cbh:instance:updateInstanceSecurityGroup	Grants the permission to update the security group of a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh::operateAuthorization	Grants the permission to create or cancel the agency authorization for the CBH service.	Write	-	-	-
cbh::getAuthorization	Grants the permission to obtain the authorization information of the CBH service from the tenant.	Read	-	-	-
cbh::listTags	Grants the permission to query all tags.	List	-	-	-
cbh:instance:getInstanceTags	Grants the permission to query tags of CBH instances.	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key	-
cbh:instance:countInstancesByTag	Grants the permission to count the number of instances that meet the tag conditions.	List	instance *	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key	Alias
cbh:instance:listInstancesByTag	Grants the permission to search for instances by tag.	List	-	-	-
cbh:instance:operateInstanceTags	Grants the permission to operate the resource tags of the CBH instance.	Tagging	instance *	• g:EnterpriseProjectId • g:ResourceTag/tag-key • g:RequestTag/tag-key • g:TagKeys	-
cbh:instance:getOmUrl	Grants the permission to obtain the URLs for O&M of assets managed in CBH.	Read	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:getOmUrl
cbh:instance:rollbackInstance	Grants the permission to roll back a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:upgrade
cbh:instance:migrateInstanceTraffic	Grants the permission to migrate traffic of a CBH instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>	cbh:instance:upgrade
cbh:instance:switchInstanceVpc	Grants the permission to switch the VPC of the bastion host instance.	Write	instance *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • cbh:VpcId • cbh:SubnetId	-

Each API of CBH usually supports one or more actions. **Table 5-168** lists the supported actions and dependencies.

Table 5-168 Actions and dependencies supported by CBH APIs

API	Action	Dependencies
GET /v2/{project_id}/cbs/available-zone	cbh::listAvailableZones	-
	cbh::getEcsQuota	ecs:cloudServerFlavors:get
	cbh::getQuota	-
GET /v2/{project_id}/cbs/instance/specification	cbh::listSpecifications	-
GET /v2/{project_id}/cbs/instance/list	cbh:instance:listInstances	eps:enterpriseProjects:list
	cbh:instance:getInstanceStatus	-
POST /v2/{project_id}/cbs/instance/start	cbh:instance:startInstance	-
POST /v2/{project_id}/cbs/instance/stop	cbh:instance:stopInstance	-
	cbh:instance:rebootInstance	-
POST /v2/{project_id}/cbs/instance/upgrade	cbh:instance:upgradeInstance	-
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	-
	cbh:instance:alterInstance	evs:quotas:get

API	Action	Dependencies
POST /v2/{project_id}/cbs/instance	cbh:instance:createInstance	• vpc:quotas:list • vpc:subnets:list • vpc:subnets:get • vpc:securityGroups:list • ecs:cloudServerFlavors:get
	cbh:instance:bindInstanceEip	-
	cbh:instance:unbindInstanceEip	-
PUT /v2/{project_id}/cbs/instance/{server_id}/security-groups	cbh:instance:updateInstanceSecurityGroup	vpc:ports:update
	cbh::operateAuthorization	-
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	-
	cbh:instance:operateInstanceTags	-
POST /v2/{project_id}/cbs/instance/{server_id}/eip/bind	cbh:instance:bindInstanceEip	• eip:publicIps:list • eip:publicIps:update
POST /v2/{project_id}/cbs/instance/{server_id}/eip/unbind	cbh:instance:unbindInstanceEip	• eip:publicIps:update • eip:publicIps:list

API	Action	Dependencies
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	-
	cbh:instance:migrateInstanceTraffic	-
POST /v2/{project_id}/cbs/instance/rollback	cbh:instance:rollbackInstance	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-169**, 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 CBH.

Table 5-169 Resource types supported by CBH

Resource Type	URN
instance	cbh:<region>:<account-id>:instance:<instance-id>

Conditions

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, cbh:) apply only to operations of EVS. For details, see **Table 5-170**.
  - 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 constitute a complete condition statement. An SCP takes effect only when the statement meets related requirements. For supported condition operators, see Operators.

The following table lists the condition keys that you can define in SCPs for CBH. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-170 Service-specific condition keys supported by CBH

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
cbh:VpcId	string	Single-valued	Controls access to a bastion host based on its VPC ID.
cbh:SubnetId	string	Single-valued	Controls access to a bastion host based on its subnet ID.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
cbh:AllowBindPublicIp	boolean	Single-valued	Grants the permissions to bind an EIP to a bastion host instance.

5.10.8.10 Database Security Service (DBSS)

The Organizations 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 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 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 DBSS, see **Resources**.
- The **Condition Key** column includes keys that you can specify in the Condition element of an SCP 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 following table lists the actions that you can define in SCP statements for DBSS.

Table 5-171 Actions supported by DBSS

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:listSqlInjectRules	Grant the permission to query SQL injection rules.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listSqls	Grant the permission to obtain the audit results.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchSqlInjectRule	Grant the permission to enable or disable the SQL injection policy.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addSqlInjectRule	Grant the permission to add custom SQL injection rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:orderSqlInjectRule	Grant the permission to sort SQL rules by priority.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:createReporter	Grant the permission to generate reports immediately.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listReporters	Grant the permission to query report information.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getRiskRuleDetail	Grant the permission to query specified risk rules.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:listAlarmEmails	Grant the permission to query alarm notification email.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:downloadReporter	Grant the permission to download reports.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listAuditScopeRules	Grant the permission to query the audit scope policy list.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addSensitiveRule	Grant the permission to add privacy data protection rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:editSensitiveRule	Grant the permission to edit privacy data protection rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteReporter	Grant the permission to delete reports.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listOperateLog	Grant the permission to query user operation logs.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listMonitorInfos	Grant the permission to query the audit instance monitoring information.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listSessionInfo	Grant the permission to query the audit instance session information.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:switchBackup	Grant the permission to enable or disable the backup function.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::downloadLicense	Grant the permission to download a sales license.	read	-	-
dbss::deleteAuditInstanceJob	Grant the permission to delete tasks failed to be created for audit instances.	write	-	-
dbss::listRdsDb	Grant the permission to query RDS databases.	list	-	-
dbss:auditInstance:instanceStart	Grant the permission to enable the audit instance.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:reboot	Grant the permission to restart the audit instance.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:stop	Grant the permission to disable the audit instance.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:upgrade	Grant the permission to upgrade the audit instance.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::queryUpgradeStatus	Grant the permission to query the upgrade status of the audit instance.	list	-	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:updateSecurityGroup	Grant the permission to modify the security group of the audit instance.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:modifyAttribute	Grant the permission to modify the audit attributes of the audit instance.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:downloadAgent	Grant the permission to download the agent.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchAgent	Grant the permission to enable or disable the agent.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listAgents	Grant the permission to query the agent list.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteAgent	Grant the permission to delete the agent.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addAgent	Grant the permission to add the agent.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:previewReporter	Grant the permission to preview a report.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:setAlarmConfig	Grant the permissions to configure alarm information.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:configAlarmEmail	Grant the permission to configure alarm notification email.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getAlarmConfig	Grant the permission to query alarm configurations.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listRiskRules	Grant the permission to query risk rules.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:exportInstancesDatabaseConfig	Grant the permission to export database configurations.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:createOnPeriod	Grant the permission to create audit instances in yearly/monthly billing mode.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
dbss:auditInstance:editSqlInjectRule	Grant the permission to edit custom SQL injection rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteSqlInjectRule	Grant the permission to delete custom SQL injection rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteSensitiveRule	Grant the permission to delete privacy data protection rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:deleteAuditScopeRule	Grant the permission to delete audit scope rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteRiskRule	Grant the permission to delete risk rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteBackup	Grant the permission to delete local backup information.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listBackups	Grant the permission to query backup information.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getBackupConfig	Grant the permission to obtain backup configuration information.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:editAuditScopeRule	Grant the permission to edit audit scope rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:instanceList	Grant the permission to query audit instance information.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:createOnDemand	Grant the permission to create audit instances in the pay-per-use billing mode.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss::listCommonInfo	Grant the permission to query public information.	list	-	-
dbss:auditInstance:listInstancesSummaryInfo	Grant the permission to query the overview of all audit instances.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::getauditInstancesSummaryTaskStatus	Grant the permission to query the task status overview.	read	-	-
dbss::updateAuditInstancesSummaryInfo	Grant the permission to update the overview of all audit instances.	write	-	-
dbss:auditInstance:setReporterConfig	Grant the permission to edit the scheduled report task configurations.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getReporterConfig	Grant the permission to obtain the scheduled report task configurations.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addBareDatabase	Grant the permission to add a user-built database.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listDatabases	Grant the permission to query the database list.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchDatabase	Grant the permission to enable or disable the database audit function.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:deleteDatabase	Grant the permission to delete a database.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addAuditScopeRule	Grant the permission to add audit scope rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchAuditScopeRule	Grant the permission to enable or disable audit scope rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addRiskRule	Grant the permission to add risk rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchRiskRule	Grant the permission to enable or disable risk rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:editRiskRule	Grant the permission to edit risk rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:setRiskRulePriority	Grant the permission to set risk rule priorities.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listStatistics	Grant the permission to query the overview of audit instances.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listSensitiveRules	Grant the permission to query privacy data masking rules.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:modifySensitiveRuleSaveResultSwitch	Grant the permission to enable or disable result set storage.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:modifySensitiveRuleAnonymizeSwitch	Grant the permission to enable or disable privacy data masking.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchSensitiveRule	Grant the permission to enable or disable privacy data protection rules.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:listAlarmItems	Grant the permission to query alarms.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:markAlarm	Grant the permission to mark alarms.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:deleteAlarm	Grant the permission to delete alarms.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:restoreBackup	Grant the permission to restore backup information.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:retryBackup	Grant the permission to retry the backup operation.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:getRiskBackupConfigInfo	Grant the permission to obtain risk export configuration information.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:switchRiskBackup	Grant the permission to enable or disable the risk export function.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss:auditInstance:getRiskBackupBucketInfo	Grant the permission to obtain the OBS buckets in risk export.	read	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:setRiskBackupBucketInfo	Grant the permission to configure the OBS bucket in risk export.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss:auditInstance:addRdsDatabase	Grant the permission to add RDS databases.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::getServerInfo	Grant the permission to obtain DBSS service information.	read	-	-
dbss::getAuditInstanceJob	Grant the permission to view the created audit instance tasks.	read	-	-
dbss:auditInstance:listJobs	Grant the permission to list the created audit instance tasks.	list	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::listObsBuckets	Grant the permission to query the OBS bucket list.	list	-	-
dbss:auditInstance:instanceDelete	Grant the permission to delete audit instances.	write	dbss:<region>:<account-id>:auditInstance:<instance-id>	-
dbss::listResourcesByTag	Grant the permission to query audit instances based on tags.	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys

Item	Description	Access Level	Resource Type (*: required)	Condition Key
dbss::tagResource	Grant the permission to add instance tags in batches.	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
dbss::unTagResource	Grant the permission to delete instance tags in batches.	tagging	-	• g:RequestTag/<tag-key> • g:TagKeys
dbss::listTags	Grant the permission to query all tags in a project.	tagging	-	-
dbss::listTagsForResource	Grant the permission to query instance tags.	tagging	-	-

Each API of DBSS usually supports one or more actions. **Table 5-172** lists the supported actions and dependencies.

Table 5-172 Actions and dependencies of DBSS APIs

API	Action	Dependency Item
POST /v1/{project_id}/{instance_id}/audit/rule/risk/switch	dbss:auditInstance:switchRiskRule	-
POST /v1/{project_id}/{instance_id}/audit/agent/switch	dbss:auditInstance:switchAgent	-
GET /v1/{project_id}/dbss/audit/quota	dbss::listCommonInfo	-

API	Action	Dependency Item
GET /v1/{project_id}/dbss/audit/specification	dbss::listCommonInfo	-
GET /v2/{project_id}/dbss/audit/availability-zone	dbss::listCommonInfo	-
POST /v1/{project_id}/{instance_id}/dbss/audit/operate-log	dbss:auditInstance:listOperateLog	-
POST /v1/{project_id}/dbss/audit/security-group	dbss:auditInstance:updateSecurityGroup	-
GET /v1/{project_id}/dbss/audit/instances	dbss:auditInstance:instanceList	-
GET /v1/{project_id}/dbss/audit/jobs/{resource_id}	dbss:auditInstance:listJobs	-
POST /v2/{project_id}/dbss/audit/charge/period/order	dbss:auditInstance:createOnPeriod	dbss::listCommonInfo
GET /v1/{project_id}/{instance_id}/dbss/audit/databases	dbss:auditInstance:listDatabases	-
POST /v1/{project_id}/{instance_id}/dbss/audit/databases/rds	dbss:auditInstance:addRdsDatabase	-
GET /v1/{project_id}/{resource_type}/tags	dbss::listTags	-
POST /v1/{project_id}/{resource_type}/resource-instances/filter	dbss::listResourcesByTag	-

API	Action	Dependency Item
POST /v1/{project_id}/{resource_type}/resource-instances/count	dbss::listResourcesByTag	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/create	dbss::tagResource	-
DELETE /v1/{project_id}/{resource_type}/{resource_id}/tags/delete	dbss::unTagResource	-
GET /v1/{project_id}/{instance_id}/dbss/audit/rule/scopes	dbss:auditInstance:listAuditScopeRules	-
POST /v1/{project_id}/{instance_id}/dbss/audit/rule/sql-injections	dbss:auditInstance:listSqlInjectRules	-
GET /v1/{project_id}/{instance_id}/dbss/audit/rule/risk	dbss:auditInstance:listRiskRules	-
GET /v1/{project_id}/{instance_id}/dbss/audit/rule/risk/{risk_id}	dbss:auditInstance:getRiskRuleDetail	-
GET /v1/{project_id}/{instance_id}/dbss/audit/sensitive/masks	dbss:auditInstance:listSensitiveRules	-

Resources

DBSS does not support resource-specific permission control in identity policies. If you want to allow access to DBSS, use the wildcard (*) for the Resource element to apply identity policies to all resources.

Table 5-173 Resource types supported by DBSS

Resource Type	URN	Condition Key
auditInstance	dbss:<region>:<account-id>:auditInstance:<instance-id>	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Conditions

DBSS does not support service-specific condition keys in identity policies. DBSS can use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.8.11 Web Application Firewall (WAF)

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 IAM custom identity policies and 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 Web Application Firewall (WAF), 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 for Web Application Firewall (WAF), see **Condition**.

The following table lists the actions that you can define in SCP statements for WAF.

Table 5-174 Actions supported by WAF

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:host:list	Grants the permission to query the protected domain name list.	list	host *	-
			-	g:EnterpriseProjectId
waf:host:create	Grants the permission to create a protected domain name.	write	host *	-
			policy	-
			certificate	-
			-	g:EnterpriseProjectId
waf:host:get	Grants the permission to query a specific protected domain name.	read	host *	g:EnterpriseProjectId
waf:host:put	Grants the permission to update a specific protected domain name.	write	host *	g:EnterpriseProjectId
			certificate	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:host:delete	Grants the permission to delete a specific protected domain name.	write	host *	g:EnterpriseProjectId
waf:sourceIp:get	Grants the permission to query back-to-source IP addresses.	read	-	-
waf:policy:list	Grants the permission to query the protection policy list.	list	policy *	-
			-	g:EnterpriseProjectId
waf:policy:create	Grants the permission to create protection policies.	write	policy *	-
			-	g:EnterpriseProjectId
waf:policy:get	Grants the permission to query a protection policy.	read	policy *	g:EnterpriseProjectId
waf:policy:put	Grants the permission to update protection policies.	write	policy *	g:EnterpriseProjectId
			host	-
waf:policy:delete	Grants the permission to delete protection policies.	write	policy *	g:EnterpriseProjectId
waf:ccRule:list	Grants the permission to query the CC attack protection rule list.	list	policy *	-
			-	g:EnterpriseProjectId
waf:ccRule:create	Grants the permission to create a CC attack protection rule.	write	policy *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:ccRule:get	Grants the permission to query a CC attack protection rule.	read	policy *	g:EnterpriseProjectId
waf:ccRule:put	Grants the permission to upgrade a CC attack protection rule.	write	policy *	g:EnterpriseProjectId
waf:ccRule:delete	Grants the permission to delete a CC attack protection rule.	write	policy *	g:EnterpriseProjectId
waf:preciseProtectionRule:list	Grants the permission to query the list of precise protection rules.	list	policy *	-
			-	g:EnterpriseProjectId
waf:preciseProtectionRule:create	Grants the permission to create a precise protection rule.	write	policy *	-
			-	g:EnterpriseProjectId
waf:preciseProtectionRule:get	Grants the permission to query a precise protection rule.	read	policy *	g:EnterpriseProjectId
waf:preciseProtectionRule:put	Grants the permission to update a precise protection rule.	write	policy *	g:EnterpriseProjectId
waf:preciseProtectionRule:delete	Grants the permission to delete a precise protection rule.	write	policy *	g:EnterpriseProjectId
waf:whiteBlackIpRule:list	Grants the permission to query the list of blacklist and whitelist rules.	list	policy *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:whiteBlackIpRule:create	Grants the permission to create an IP address blacklist or whitelist.	write	policy *	-
			-	g:EnterpriseProjectId
waf:whiteBlackIpRule:get	Grants the permission to query a blacklist or whitelist rule.	read	policy *	g:EnterpriseProjectId
waf:whiteBlackIpRule:put	Grants the permission to update a blacklist or whitelist rule.	write	policy *	g:EnterpriseProjectId
waf:whiteBlackIpRule:delete	Grants the permission to delete a blacklist or whitelist rule.	write	policy *	g:EnterpriseProjectId
waf:privacyRule:list	Grants the permission to query the list of data masking rules.	list	policy *	-
			-	g:EnterpriseProjectId
waf:privacyRule:create	Grants the permission to create a data masking rule.	write	policy *	-
			-	g:EnterpriseProjectId
waf:privacyRule:get	Grants the permission to query a data masking rule.	read	policy *	g:EnterpriseProjectId
waf:privacyRule:put	Grants the permission to update a data masking rule.	write	policy *	g:EnterpriseProjectId
waf:privacyRule:delete	Grants the permission to delete a data masking rule.	write	policy *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:falseAlarmMaskRule:list	Grants the permission to query the list of false alarm masking rules.	list	policy *	-
			-	g:EnterpriseProjectId
waf:falseAlarmMaskRule:create	Grants the permission to create a false alarm masking rule.	write	policy *	-
			-	g:EnterpriseProjectId
waf:falseAlarmMaskRule:get	Grants the permission to query a false alarm masking rule.	read	policy *	g:EnterpriseProjectId
waf:falseAlarmMaskRule:put	Grants the permission to update a false alarm masking rule.	write	policy *	g:EnterpriseProjectId
waf:falseAlarmMaskRule:delete	Grants the permission to delete a false alarm masking rule.	write	policy *	g:EnterpriseProjectId
waf:geoIpRule:list	Grants the permission to query the list of geolocation access control rules.	list	policy *	-
			-	g:EnterpriseProjectId
waf:geoIpRule:create	Grants the permission to create a geolocation access control rule.	write	policy *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:geoIpRule:get	Grants the permission to query a geolocation access control rule.	read	policy *	g:EnterpriseProjectId
waf:geoIpRule:put	Grants the permission to update a geolocation access control rule.	write	policy *	g:EnterpriseProjectId
waf:geoIpRule:delete	Grants the permission to delete a geolocation access control rule.	write	policy *	g:EnterpriseProjectId
waf:antiTamperRule:list	Grants the permission to query the list of web tamper protection rules.	list	policy *	-
			-	g:EnterpriseProjectId
waf:antiTamperRule:create	Grants the permission to create a web tamper protection rule.	write	policy *	-
			-	g:EnterpriseProjectId
waf:antiTamperRule:get	Grants the permission to query a web tamper protection rule.	read	policy *	g:EnterpriseProjectId
waf:antiTamperRule:put	Grants the permission to update a web tamper protection rule.	write	policy *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:antiTamperRule:delete	Grants the permission to delete a web tamper protection rule.	write	policy *	g:EnterpriseProjectId
waf:antiLeakageRule:list	Grants the permission to query the list of information leakage prevention rules.	list	policy *	-
			-	g:EnterpriseProjectId
waf:antiLeakageRule:create	Grants the permission to create an information leakage prevention rule.	write	policy *	-
			-	g:EnterpriseProjectId
waf:antiLeakageRule:get	Grants the permission to query an information leakage prevention rule.	read	policy *	g:EnterpriseProjectId
waf:antiLeakageRule:put	Grants the permission to update an information leakage prevention rule.	write	policy *	g:EnterpriseProjectId
waf:antiLeakageRule:delete	Grants the permission to delete an information leakage prevention rule.	write	policy *	g:EnterpriseProjectId
waf:anticrawlerRule:list	Grants the permission to query the list of anti-crawler rules.	list	policy *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:anticrawlerRule:create	Grants the permission to create an anti-crawler rule.	write	policy *	-
			-	g:EnterpriseProjectId
waf:anticrawlerRule:get	Grants the permission to query an anti-crawler rule.	read	policy *	g:EnterpriseProjectId
waf:anticrawlerRule:put	Grants the permission to update an anti-crawler rule.	write	policy *	g:EnterpriseProjectId
waf:anticrawlerRule:delete	Grants the permission to delete an anti-crawler rule.	write	policy *	g:EnterpriseProjectId
waf:punishmentRule:list	Grants the permission to query the list of known attack source rules.	list	policy *	-
			-	g:EnterpriseProjectId
waf:punishmentRule:create	Grants the permission to create a known attack source rule.	write	policy *	-
			-	g:EnterpriseProjectId
waf:punishmentRule:get	Grants the permission to query a known attack source rule.	read	policy *	g:EnterpriseProjectId
waf:punishmentRule:put	Grants the permission to update a known attack source rule.	write	policy *	g:EnterpriseProjectId
waf:punishmentRule:delete	Grants the permission to delete a known attack source rule.	write	policy *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:valueList:list	Grants the permission to query the list of reference tables.	list	-	g:EnterpriseProjectId
waf:valueList:create	Grants the permission to create a reference table.	write	-	g:EnterpriseProjectId
waf:valueList:get	Grants the permission to query a reference table.	read	-	g:EnterpriseProjectId
waf:valueList:put	Grants the permission to update a reference table.	write	-	g:EnterpriseProjectId
waf:valueList:delete	Grants the permission to delete a reference table.	write	-	g:EnterpriseProjectId
waf:ipgroup:list	Grants permission to query IP address groups.	list	-	g:EnterpriseProjectId
waf:ipgroup:create	Grants permission to create an IP address group.	write	-	g:EnterpriseProjectId
waf:ipgroup:get	Grants the permission to query an IP address group.	read	-	g:EnterpriseProjectId
waf:ipgroup:put	Grants permission to modify an IP address group.	write	-	g:EnterpriseProjectId
waf:ipgroup:delete	Grants permission to delete an IP address group.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:certificate:list	Grants the permission to query the certificate list.	list	certificate *	-
			-	g:EnterpriseProjectId
waf:certificate:create	Grants permission to add a certificate.	write	certificate *	-
			-	g:EnterpriseProjectId
waf:certificate:get	Grants the permission to query a certificate.	read	certificate *	g:EnterpriseProjectId
waf:certificate:put	Grants the permission to modify a certificate in WAF.	write	certificate *	g:EnterpriseProjectId
waf:certificate:delete	Delete a certificate.	write	certificate *	g:EnterpriseProjectId
waf:certificate:apply	Grants the permission to apply a certificate to a domain name.	write	certificate *	g:EnterpriseProjectId
			host *	-
waf:premiumInstance:list	Grants the permission to query the dedicated engine instance list.	list	premiumInstance *	-
			-	g:EnterpriseProjectId
waf:premiumInstance:create	Grants the permission to create a dedicated engine instance.	write	premiumInstance *	-
			-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:premiumInstance:get	Grants the permission to query a dedicated engine instance.	read	premiumInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
waf:premiumInstance:put	Grants the permission to update a dedicated engine instance.	write	premiumInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
waf:premiumInstance:delete	Grants the permission to delete a dedicated engine instance.	write	premiumInstance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
waf:event:get	Grants the permission to query protection events.	read	-	g:EnterpriseProjectId
waf:ltsConfig:get	Grants the permission to query the configuration of the interconnection with LTS.	list	-	g:EnterpriseProjectId
waf:ltsConfig:put	Grants the permission to update the configuration of the interconnection with LTS.	write	-	g:EnterpriseProjectId
waf:postpaid:create	Grants the permission to enable the pay-per-use billing mode.	write	-	g:EnterpriseProjectId
waf:postpaid:delete	Grants the permission to disable pay-per-use billing.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
waf:prepaid:create	Grants the permission to create a yearly/ monthly order.	write	-	• g:EnterpriseProjectId • g:RequestTag/ <tag-key> • g:TagKeys
waf:subscription:get	Grants the permission to query subscriptions to the cloud mode.	read	-	-
waf:alert:get	Grants the permission to query alarm notification configurations.	list	-	-
waf:alert:put	Grants the permission to update alarm notification configurations.	write	-	-
waf:consoleConfig:get	Grants the permission to query the console configurations.	read	-	-

A WAF API usually has one or more actions. **Table 5-175** lists the supported actions and dependencies.

Table 5-175 Actions and dependencies supported by CCE APIs

API	Action	Dependencies
POST /v1/ {project_id}/waf/ instance	waf:host:create	-
DELETE /v1/ {project_id}/waf/ instance/ {instance_id}	waf:host:delete	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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}/antitamper/{rule_id}/refresh	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	-

API	Action	Dependencies
POST /v1/{project_id}/waf/policy/{policy_id}/punishment	waf:punishmentRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/geoip	waf:geoIpRule:create	-
POST /v1/{project_id}/waf/policy/{policy_id}/ignore	waf:falseAlarmMaskRule:create	-
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	-

API	Action	Dependencies
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	-
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:preciseProtection-Rule: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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
PUT /v1/{project_id}/waf/policy/{policy_id}/geoip/{rule_id}	waf:geoIpRule:put	-
-	waf:antiTamperRule:put	-
PUT /v1/{project_id}/waf/policy/{policy_id}/antileakage/{rule_id}	waf:antiLeakageRule:put	-
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	-

API	Action	Dependencies
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	-
GET /v1/{project_id}/waf/policy/{policy_id}/custom/{rule_id}	waf:preciseProtectionRule: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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
POST /v1/{project_id}/premium-waf/instance	waf:premiumInstance:create	-
DELETE /v1/{project_id}/premium-waf/instance/{instance_id}	waf:premiumInstance:delete	-
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	-

API	Action	Dependencies
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	-
PUT /v2/{project_id}/waf/alert/{alert_id}	waf:alert:put	-
GET /v1/{project_id}/waf/config/source-ip	waf:sourceIp:get	-
POST /v1/{project_id}/composite-waf/hosts/migration	waf:host:create	-
GET /v1/{project_id}/composite-waf/host	waf:host:list	-
GET /v1/{project_id}/composite-waf/host/{host_id}	waf:host:get	-

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-176**, 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.

WAF defines the following resource types that can be used in the Resource element of a custom SCP.

Table 5-176 Resource types supported by WAF

Resource Type	URN
policy	waf:<region>:<account-id>:policy:<policy-id>

Resource Type	URN
host	waf:<region>:<account-id>:host:<host-id>
premiumInstance	waf:<region>:<account-id>:premiumInstance:<instance-id>
certificate	waf:<region>:<account-id>:certificate:<certificate-id>

Condition

WAF does not support service-level condition keys in an SCP. WAF can use global condition keys that are applicable to all services. For details, see Global Condition Keys.

5.10.9 Internet of Things

5.10.9.1 IoT Device Access (IoTDA)

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 IoTDA, 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 condition keys defined by IoTDA, see **Conditions**.

The following table lists the actions that you can define in SCP statements for IoTDA.

Table 5-177 Actions supported by IoTDA

Action	Description	Access Level	Resource Type	Condition Key
iotda:products:create	Creating a product	write	app	g:EnterpriseProjectId
iotda:products:queryList	Querying the product list	list	app	g:EnterpriseProjectId
iotda:products:query	Querying a product	read	app	g:EnterpriseProjectId
iotda:products:modify	Modifying a product	write	app	g:EnterpriseProjectId
iotda:products:delete	Deleting a product	write	app	g:EnterpriseProjectId
iotda:devices:register	Creating a device	write	app	g:EnterpriseProjectId
iotda:devices:queryList	Querying the device list	list	app	g:EnterpriseProjectId
iotda:devices:query	Querying a device	read	app	g:EnterpriseProjectId
iotda:devices:modify	Modifying a device	write	app	g:EnterpriseProjectId
iotda:devices:delete	Deleting a device	write	app	g:EnterpriseProjectId
iotda:devices:resetSecret	Resetting a device secret	write	app	g:EnterpriseProjectId
iotda:devices:freeze	Freezing a device	write	app	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
iotda:devices:unfreeze	Unfreezing a device	write	app	g:EnterpriseProjectId
iotda:devices:resetFingerprint	Resetting a device fingerprint	write	app	g:EnterpriseProjectId
iotda:devices:queryList	Querying device list flexibly	list	app	g:EnterpriseProjectId
iotda:messages:send	Delivering a device message	write	app	g:EnterpriseProjectId
iotda:messages:queryList	Querying device messages	list	app	g:EnterpriseProjectId
iotda:messages:query	Query a message by message ID	read	app	g:EnterpriseProjectId
iotda:message:broadcast	Broadcasting a message	write	app	g:EnterpriseProjectId
iotda:commands:send	Delivering a device command	write	app	g:EnterpriseProjectId
iotda:asynccommands:send	Delivering an asynchronous command	write	app	g:EnterpriseProjectId
iotda:asynccommands:query	Querying a command with a specific ID	read	app	g:EnterpriseProjectId
iotda:properties:modify	Modifying device properties	write	app	g:EnterpriseProjectId
iotda:properties:query	Querying device properties	read	app	g:EnterpriseProjectId
iotda:shadow:query	Querying device shadow data	read	app	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
iotda:shadow:config	Configuring desired device shadow data	write	app	g:EnterpriseProjectId
iotda:amqpqueue:create	Creating an AMQP queue	write	-	g:EnterpriseProjectId
iotda:amqpqueue:queryList	Querying the AMQP list	list	-	g:EnterpriseProjectId
iotda:amqpqueue:query	Querying an AMQP queue	read	-	g:EnterpriseProjectId
iotda:amqpqueue:delete	Deleting an AMQP queue	write	-	g:EnterpriseProjectId
iotda:accesscode:create	Generating an access credential	write	-	g:EnterpriseProjectId
iotda:routingrules:create	Creating a rule triggering condition	write	app	g:EnterpriseProjectId
iotda:routingrules:queryList	Querying the rule triggering condition list	list	app	g:EnterpriseProjectId
iotda:routingrules:query	Querying a rule triggering condition	read	app	g:EnterpriseProjectId
iotda:routingrules:modify	Modifying a rule triggering condition	write	app	g:EnterpriseProjectId
iotda:routingrules:delete	Deleting a rule triggering condition	write	app	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
iotda:routingactions:create	Creating a rule action	write	app	• g:EnterpriseProjectId • iotda:HttpForwardingEnableSSL • iotda:HttpForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableSSL • iotda:MysqlForwardingEnableSSL • iotda:MRSKafkaForwardingEnableAuthentication • iotda:DMSRocketMQForwardingEnableSSL • iotda:MongoDBForwardingEnableSSL
iotda:routingactions:queryList	Querying the rule action list	list	app	g:EnterpriseProjectId
iotda:routingactions:query	Querying a rule action	read	app	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
iotda:routingactions:modify	Modifying a rule action	write	app	• g:EnterpriseProjectId • iotda:HttpForwardingEnableSSL • iotda:HttpForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableAuthentication • iotda:DMSKafkaForwardingEnableSSL • iotda:MysqlForwardingEnableSSL • iotda:MRSKafkaForwardingEnableAuthentication • iotda:DMSRocketMQForwardingEnableSSL • iotda:MongoDBForwardingEnableSSL
iotda:routingactions:delete	Deleting a rule action	write	app	g:EnterpriseProjectId
iotda:rules:create	Creating a rule	write	-	g:EnterpriseProjectId
iotda:rules:queryList	Querying the rule list	list	-	g:EnterpriseProjectId
iotda:rules:modify	Modifying a rule	write	-	g:EnterpriseProjectId
iotda:rules:query	Querying a rule	read	-	g:EnterpriseProjectId
iotda:rules:delete	Deleting a rule	write	-	g:EnterpriseProjectId
iotda:rules:modifyStatus	Modifying the rule status	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
iotda:group:create	Adding a device group	write	app	g:EnterpriseProjectId
iotda:group:queryList	Querying the device group list	list	app	g:EnterpriseProjectId
iotda:group:query	Querying a device group	read	app	g:EnterpriseProjectId
iotda:group:modify	Modifying a device group	write	app	g:EnterpriseProjectId
iotda:group:delete	Deleting a device group	write	app	g:EnterpriseProjectId
iotda:group:addDevice	Managing devices in a device group	write	app	g:EnterpriseProjectId
iotda:group:queryDeviceList	Query devices in a device group	list	app	g:EnterpriseProjectId
iotda:tags:bind	Binding a tag	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
iotda:tags:unbind	Unbinding a tag	tagging	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
iotda:tags:queryResourceList	Querying resources by tag	list	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
iotda:apps:queryList	Querying the resource space list	list	app	g:EnterpriseProjectId
iotda:app:create	Creating a resource space	write	app	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
iotda:apps:query	Querying a resource space	read	app	g:EnterpriseProjectId
iotda:apps:delete	Deleting a resource space	write	app	g:EnterpriseProjectId
iotda:batchtasks:create	Creating a batch task	write	-	g:EnterpriseProjectId
iotda:batchtasks:queryList	Querying the batch task list	list	-	g:EnterpriseProjectId
iotda:batchtasks:query	Querying a batch task	read	-	g:EnterpriseProjectId
iotda:batchtasks:retry	Retrying a batch task	write	-	g:EnterpriseProjectId
iotda:batchtasks:stop	Stopping a batch task	write	-	g:EnterpriseProjectId
iotda:batchtasks:delete	Deleting a batch task	write	-	g:EnterpriseProjectId
iotda:batchtaskfiles:create	Uploading a batch task file	write	-	g:EnterpriseProjectId
iotda:batchtaskfiles:queryList	Querying the list of batch task files	list	-	g:EnterpriseProjectId
iotda:batchtaskfiles:delete	Deleting a batch task file	write	-	g:EnterpriseProjectId
iotda:certificates:upload	Uploading a device CA certificate	write	app	g:EnterpriseProjectId
iotda:certificates:queryList	Obtaining the device CA certificate list	list	app	g:EnterpriseProjectId
iotda:certificates:delete	Deleting a device CA certificate	write	app	g:EnterpriseProjectId
iotda:certificates:check	Verifying a device CA certificate	write	app	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
iotda:otapackages:create	Creating an OTA upgrade package	write	-	g:EnterpriseProjectId
iotda:otapackages:queryList	Querying the OTA upgrade package list	list	-	g:EnterpriseProjectId
iotda:otapackages:query	Obtaining OTA upgrade package details	read	-	g:EnterpriseProjectId
iotda:otapackages:delete	Deleting an OTA upgrade package	write	-	g:EnterpriseProjectId
iotda:tunnel:queryList	Querying the tunnel list	list	-	g:EnterpriseProjectId
iotda:tunnel:create	Creating a device tunnel	write	-	• g:EnterpriseProjectId • iotda:DeviceGroupId
iotda:tunnel:delete	Deleting a device tunnel	write	-	g:EnterpriseProjectId
iotda:tunnel:query	Querying tunnel details	read	-	g:EnterpriseProjectId
iotda:tunnel:update	Modifying a device tunnel	write	-	g:EnterpriseProjectId
iotda:instance:create	Creating an Instance	write	-	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>
iotda:instance:update	Modifying an Instance	write	-	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • iotda:AllowPublicAccess • iotda:AllowPublicForwarding • iotda:DomainConfiguration

Action	Description	Access Level	Resource Type	Condition Key
iotda:instance:query	Querying instance details	read	instance	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
iotda:instance:queryList	Querying the Instance List	read	-	-
iotda:instance:delete	Deleting an instance	write	instance	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
iotda:instance:operateTag	Performing operations on instance tags	write	instance	• g:EnterpriseProjectId • g:TagKeys • g:RequestTag/<tag-key>

Each API of IoTDA usually supports one or more actions. **Table 2** lists the supported actions and dependencies.

Table 5-178 Actions and dependencies supported by IoTDA APIs

API	Action	Dependencies
POST /v5/iot/{project_id}/products	iotda:products:create	-
GET /v5/iot/{project_id}/products	iotda:products:queryList	-
GET /v5/iot/{project_id}/products/{product_id}	iotda:products:query	-
PUT /v5/iot/{project_id}/products/{product_id}	iotda:products:modify	-
DELETE /v5/iot/{project_id}/products/{product_id}	iotda:products:delete	-
POST /v5/iot/{project_id}/devices	iotda:devices:register	-
GET /v5/iot/{project_id}/devices	iotda:devices:queryList	-
GET /v5/iot/{project_id}/devices/{device_id}	iotda:devices:query	-
PUT /v5/iot/{project_id}/devices/{device_id}	iotda:devices:modify	-

API	Action	Dependencies
DELETE /v5/iot/{project_id}/devices/{device_id}	iotda:devices:delete	-
POST /v5/iot/{project_id}/devices/{device_id}/action	iotda:devices:resetSecret	-
POST /v5/iot/{project_id}/devices/{device_id}/freeze	iotda:devices:freeze	-
POST /v5/iot/{project_id}/devices/{device_id}/unfreeze	iotda:devices:unfreeze	-
POST /v5/iot/{project_id}/devices/{device_id}/reset-fingerprint	iotda:devices:resetFingerprint	-
POST /v5/iot/{project_id}/search/query-devices	iotda:devices:queryList	-
POST /v5/iot/{project_id}/devices/{device_id}/messages	iotda:messages:send	-
GET /v5/iot/{project_id}/devices/{device_id}/messages	iotda:messages:queryList	-
GET /v5/iot/{project_id}/devices/{device_id}/messages/{message_id}	iotda:messages:query	-
POST /v5/iot/{project_id}/broadcast-messages	iotda:message:broadcast	-
POST /v5/iot/{project_id}/devices/{device_id}/commands	iotda:commands:send	-
POST /v5/iot/{project_id}/devices/{device_id}/async-commands	iotda:asynccommands:send	-
GET /v5/iot/{project_id}/devices/{device_id}/async-commands/{command_id}	iotda:asynccommands:query	-
PUT /v5/iot/{project_id}/devices/{device_id}/properties	iotda:properties:modify	-
GET /v5/iot/{project_id}/devices/{device_id}/properties	iotda:properties:query	-
GET /v5/iot/{project_id}/devices/{device_id}/shadow	iotda:shadow:query	-
PUT /v5/iot/{project_id}/devices/{device_id}/shadow	iotda:shadow:config	-
POST /v5/iot/{project_id}/amqp-queues	iotda:amqpqueue:create	-

API	Action	Dependencies
GET /v5/iot/{project_id}/amqp-queues	iotda:amqpqueue:queryList	-
GET /v5/iot/{project_id}/amqp-queues/{queue_id}	iotda:amqpqueue:query	-
DELETE /v5/iot/{project_id}/amqp-queues/{queue_id}	iotda:amqpqueue:delete	-
POST /v5/iot/{project_id}/auth/accesscode	iotda:accesscode:create	-
POST /v5/iot/{project_id}/routing-rule/rules	iotda:routingrules:create	-
GET /v5/iot/{project_id}/routing-rule/rules	iotda:routingrules:queryList	-
GET /v5/iot/{project_id}/routing-rule/rules/{rule_id}	iotda:routingrules:query	-
PUT /v5/iot/{project_id}/routing-rule/rules/{rule_id}	iotda:routingrules:modify	-
DELETE /v5/iot/{project_id}/routing-rule/rules/{rule_id}	iotda:routingrules:delete	-
POST /v5/iot/{project_id}/routing-rule/actions	iotda:routingactions:create	-
GET /v5/iot/{project_id}/routing-rule/actions	iotda:routingactions:queryList	-
GET /v5/iot/{project_id}/routing-rule/actions/{action_id}	iotda:routingactions:query	-
PUT /v5/iot/{project_id}/routing-rule/actions/{action_id}	iotda:routingactions:modify	-
DELETE /v5/iot/{project_id}/routing-rule/actions/{action_id}	iotda:routingactions:delete	-
POST /v5/iot/{project_id}/rules	iotda:rules:create	-
GET /v5/iot/{project_id}/rules	iotda:rules:queryList	-
PUT /v5/iot/{project_id}/rules/{rule_id}	iotda:rules:modify	-
GET /v5/iot/{project_id}/rules/{rule_id}	iotda:rules:query	-
DELETE /v5/iot/{project_id}/rules/{rule_id}	iotda:rules:delete	-
PUT /v5/iot/{project_id}/rules/{rule_id}/status	iotda:rules:modifyStatus	-
POST /v5/iot/{project_id}/device-group	iotda:group:create	-

API	Action	Dependencies
GET /v5/iot/{project_id}/device-group	iotda:group:queryList	-
GET /v5/iot/{project_id}/device-group/{group_id}	iotda:group:query	-
PUT /v5/iot/{project_id}/device-group/{group_id}	iotda:group:modify	-
DELETE /v5/iot/{project_id}/device-group/{group_id}	iotda:group:delete	-
POST /v5/iot/{project_id}/device-group/{group_id}/action	iotda:group:addDevice	-
GET /v5/iot/{project_id}/device-group/{group_id}/devices	iotda:group:queryDeviceList	-
POST /v5/iot/{project_id}/tags/bind-resource	iotda:tags:bind	-
POST /v5/iot/{project_id}/tags/unbind-resource	iotda:tags:unbind	-
POST /v5/iot/{project_id}/tags/query-resources	iotda:tags:queryResourceList	-
GET /v5/iot/{project_id}/apps	iotda:apps:queryList	-
POST /v5/iot/{project_id}/apps	iotda:app:create	-
GET /v5/iot/{project_id}/apps/{app_id}	iotda:apps:query	-
DELETE /v5/iot/{project_id}/apps/{app_id}	iotda:apps:delete	-
POST /v5/iot/{project_id}/batchtasks	iotda:batchtasks:create	-
GET /v5/iot/{project_id}/batchtasks	iotda:batchtasks:queryList	-
GET /v5/iot/{project_id}/batchtasks/{task_id}	iotda:batchtasks:query	-
POST /v5/iot/{project_id}/batchtasks/{task_id}/retry	iotda:batchtasks:retry	-
POST /v5/iot/{project_id}/batchtasks/{task_id}/stop	iotda:batchtasks:stop	-
DELETE /v5/iot/{project_id}/batchtasks/{task_id}	iotda:batchtasks:delete	-
POST /v5/iot/{project_id}/batchtask-files	iotda:batchtaskfiles:create	-
GET /v5/iot/{project_id}/batchtask-files	iotda:batchtaskfiles:queryList	-

API	Action	Dependencies
DELETE /v5/iot/{project_id}/batchtask-files/{file_id}	iotda:batchtaskfiles:delete	-
POST /v5/iot/{project_id}/certificates	iotda:certificates:upload	-
GET /v5/iot/{project_id}/certificates	iotda:certificates:queryList	-
DELETE /v5/iot/{project_id}/certificates/{certificate_id}	iotda:certificates:delete	-
POST /v5/iot/{project_id}/certificates/{certificate_id}/action	iotda:certificates:check	-
POST /v5/iot/{project_id}/ota-upgrades/packages	iotda:otapackages:create	-
GET /v5/iot/{project_id}/ota-upgrades/packages	iotda:otapackages:queryList	-
GET /v5/iot/{project_id}/ota-upgrades/packages/{package_id}	iotda:otapackages:query	-
DELETE /v5/iot/{project_id}/ota-upgrades/packages/{package_id}	iotda:otapackages:delete	-
GET /v5/iot/{project_id}/tunnels	iotda:tunnel:queryList	-
POST /v5/iot/{project_id}/tunnels	iotda:tunnel:create	-
DELETE /v5/iot/{project_id}/tunnels/{id}	iotda:tunnel:delete	-
GET /v5/iot/{project_id}/tunnels/{id}	iotda:tunnel:query	-
PUT /v5/iot/{project_id}/tunnels/{id}	iotda:tunnel:update	-
POST /v5/iot/{project_id}/iotda-instances	iotda:instance:create	-
PUT /v5/iot/{project_id}/iotda-instances/{instance_id}	iotda:instance:update	-
GET /v5/iot/{project_id}/iotda-instances/{instance_id}	iotda:instance:query	-
GET /v5/iot/{project_id}/iotda-instances	iotda:instance:queryList	-
DELETE /v5/iot/{project_id}/iotda-instances/{instance_id}	iotda:instance:delete	-
POST /v5/iot/{project_id}/iotda-instances/{instance_id}/bind-tags	iotda:instance:operateTag	-

API	Action	Dependencies
POST /v5/iot/{project_id}/iotda-instances/{instance_id}/unbind-tags	iotda:instance:operateTag	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-179**, 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.

Table 5-179 Resource types supported by IoTDA

Resource Type	URN
app	iotda:<region>:<account-id>:app:<app-id>
instance	iotda:<region>:<account-id>:instance:<instance-id>

Conditions

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, IoTDA:) apply only to operations of the service. For details, see **Table 5-180**.
  - 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.

The following table lists the condition keys that you can define in SCPs for IoTDA. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-180 Condition keys supported by IoTDA

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
iotda:AllowPublicAccess	Boolean	Single-valued	Filters requests based on the configuration that is set during instance modification. Condition: allowing public network access.
iotda:AllowPublicForwarding	Boolean	Single-valued	Filters requests based on the configuration that is set during instance modification. Condition: allowing public network forwarding.
iotda:DomainConfiguration	Boolean	Single-valued	Filters requests based on the configuration that is set during instance modification. Condition: domain names.
iotda:DeviceGroupId	String	Single-valued	Filters requests based on the configuration that is set during tunnel creation. Condition: device associated groups.
iotda:HttpForwardingEnableSSL	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling the TLS protocol for HTTP channels.
iotda:HttpForwardingEnableAuthentication	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling token authentication for HTTP channels.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
iotda:DMSKafkaForwardingEnableAuthentication	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling SCRAM-SHA-512 mechanism for Distributed Message Service (DMS) Kafka channels.
iotda:DMSKafkaForwardingEnableSSL	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling the TLS protocol for DMS Kafka channels.
iotda:MysqlForwardingEnableSSL	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling the TLS protocol for MySQL channels.
iotda:MRSKafkaForwardingEnableAuthentication	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling Kerberos authentication for MapReduce Service (MRS) Kafka channels.
iotda:DMSRocketMQForwardingEnableSSL	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling the TLS protocol for RocketMQ channels.
iotda:MongoDBForwardingEnableSSL	Boolean	Single-valued	Filters requests based on the configuration that is set during rule action creation/ modification. Condition: enabling the TLS protocol for MongoDB channels.

5.10.10 Middleware

5.10.10.1 Distributed Cache Service (DCS)

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 DCS, 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 DCS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for DCS.

Table 5-181 Actions supported by DCS

Action	Description	Access Level	Resource Type (* required)	Condition Key
dcs:instance:create	Grants permission to create DCS instances.	write	-	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys • dcs:backupEnabled
dcs:instance:list	Grants permission to list DCS instances.	list	-	g:EnterpriseProjectId
dcs:instance:exportListFile	Grants permission to download the exported DCS instance list file.	list	-	-
dcs:instance:delete	Grants permission to delete DCS instances.	write	instance	g:EnterpriseProjectId
dcs:instance:get	Grants permission to query DCS instances.	read	instance *	g:EnterpriseProjectId
dcs:instance:modify	Grants permission to modify DCS instances.	write	instance *	• g:EnterpriseProjectId • dcs:backupEnabled
dcs:instance:scale	Grants permission to increase DCS instance specifications.	write	instance *	g:EnterpriseProjectId
dcs:instance:swap	Grants permission to perform master/replica switchovers on DCS instances.	write	instance *	g:EnterpriseProjectId
dcs:instance:modifyAuthInfo	Grants permission to modify the passwords of DCS instances.	write	instance *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
dcs:instance:modifyStatus	Grants permission to restart DCS instances or clear their data.	write	instance *	g:EnterpriseProjectId
dcs:instance:getConfiguration	Grants permission to query DCS instance configuration parameters.	read	instance *	g:EnterpriseProjectId
dcs:instance:modifyConfiguration	Grants permission to modify DCS instance configuration parameters.	write	instance *	g:EnterpriseProjectId
dcs:instance:deleteDataBackupFile	Grants permission to delete DCS instance backup data.	write	instance *	g:EnterpriseProjectId
dcs:instance:restoreData	Grants permission to restore DCS instance data.	write	instance *	g:EnterpriseProjectId
dcs:instance:getDataRestoreLog	Grants permission to query DCS instance restoration records.	read	instance *	g:EnterpriseProjectId
dcs:instance:downloadBackupData	Grants permission to obtain backup file URLs.	read	instance *	g:EnterpriseProjectId
dcs:instance:backupData	Grants permission to back up DCS instance data.	write	instance *	g:EnterpriseProjectId
dcs:instance:getDataBackupLog	Grants permission to query DCS instance backup records.	read	instance *	g:EnterpriseProjectId
dcs:migrationTask:create	Grants permission to create data migration tasks.	write	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
dcs:migrationTask:list	Grants permission to list data migration tasks.	list	-	-
dcs:migrationTask:delete	Grants permission to delete data migration tasks.	write	migrationTask	-
dcs:migrationTask:get	Grants permission to query data migration tasks.	read	migrationTask *	-
dcs:migrationTask:modify	Grants permission to configure and stop data migration tasks.	write	migrationTask *	-
dcs:instance:listBigKey	Grants permission to query big keys.	list	instance *	g:EnterpriseProjectId
dcs:instance:getBigKey	Grants permission to query big key details.	read	instance *	g:EnterpriseProjectId
dcs:instance:deleteBigKeyScanTask	Grants permission to delete big key scan tasks.	write	instance	g:EnterpriseProjectId
dcs:instance:updateBigKeyAutoScan-Config	Grants permission to reconfigure big key scan tasks.	write	instance *	g:EnterpriseProjectId
dcs:instance:getBigKeyAutoScanConfig	Grants permission to query configurations of big key scan tasks.	read	instance *	g:EnterpriseProjectId
dcs:instance:analyzeHotKey	Grants permission to perform hot key analysis.	write	instance *	g:EnterpriseProjectId
dcs:instance:listHotKey	Grants permission to list hot keys.	list	instance *	g:EnterpriseProjectId
dcs:instance:getHotKey	Grants permission to query hot key details.	read	instance *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (* required)	Condition Key
dcs:instance:deleteHotKeyScanTask	Grants permission to delete hot key scan tasks.	write	instance	g:EnterpriseProjectId
dcs:instance:updateHotKeyAutoScanConfig	Grants permission to reconfigure hot key scan tasks.	write	instance *	g:EnterpriseProjectId
dcs:instance:getHotKeyAutoScanConfig	Grants permission to query configurations of hot key scan tasks.	read	instance *	g:EnterpriseProjectId
dcs:instance:analyzeExpiredKey	Grants permission to perform expired key analysis.	write	instance *	g:EnterpriseProjectId
dcs:instance:getAutoExpiredKeyScan-Task	Grants permission to query expired key scan tasks.	read	instance *	-
dcs:instance:updateExpiredKeyScan-Config	Grants permission to reconfigure expired key scan tasks.	write	instance *	g:EnterpriseProjectId
dcs:instance:getExpiredKeyScanCon-fig	Grants permission to query configurations of expired key scan tasks.	read	instance *	g:EnterpriseProjectId
dcs:slowlog:list	Grants permission to query slow query logs.	list	instance *	g:EnterpriseProjectId
dcs:aclaccount:create	Grants permission to create ACL accounts.	write	instance *	-
dcs:aclaccount:list	Grants permission to query ACL accounts.	list	instance *	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
dcs:aclaccount:modify	Grants permission to modify the passwords of ACL accounts.	write	instance *	-
dcs:aclaccount:delete	Grants permission to delete ACL accounts.	write	instance *	-
dcs:whitelist:modify	Grants permission to configure IP address whitelist groups.	write	instance *	-
dcs:whitelist:list	Grants permission to query the IP address whitelist of instances.	list	instance *	-
dcs:instance:getBackgroundTask	Grants permission to query background tasks.	read	instance *	g:EnterpriseProjectId
dcs:instance:deleteBackgroundTask	Grants permission to delete background tasks.	write	instance *	g:EnterpriseProjectId
dcs:instance:createDiagnosisTask	Grants permission to diagnose instances.	write	instance *	g:EnterpriseProjectId
dcs:instance:listDiagnosisTask	Grants permission to query diagnosis tasks.	list	instance *	g:EnterpriseProjectId
dcs:instance:getDiagnosisTask	Grants permission to query diagnosis details.	read	instance *	g:EnterpriseProjectId
dcs:instance:deleteDiagnosisTask	Grants permission to delete diagnosis records.	write	instance *	g:EnterpriseProjectId
dcs:template:list	Grants permission to list parameter templates.	list	-	-
dcs:template:create	Grants permission to customize templates.	write	-	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
dcs:template:get	Grants permission to query parameter templates.	read	-	-
dcs:template:modify	Grants permission to modify custom templates.	write	-	-
dcs:template:delete	Grants permission to delete custom templates.	write	-	-
dcs:tag:list	Grants permission to query all tags in your tenant account.	list	-	-
dcs:tag:modify	Grants permission to add or delete tags in batches.	write	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcs:tag:get	Grants permission to query tags of an instance.	read	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
dcs:redisLog:get	Grants permission to obtain log download URLs.	read	instance *	-
dcs:quota:get	Grants permission to query tenant quotas.	read	-	-
dcs:instance:webcli	Grants permission to connect to DCS Redis instances using Web CLI.	write	instance *	-
dcs:clientIpTrans:modify	Grants permission to enable or disable client IP pass-through.	write	instance *	-

Action	Description	Access Level	Resource Type (* required)	Condition Key
dcs:clients:list	Grants permission to list Redis sessions.	read	instance *	-
dcs:clients:kill	Grants permission to kill Redis sessions.	write	instance *	-
dcs:ssl:get	Grants permissions to obtain SSL certificate information.	read	instance *	-
dcs:ssl:modify	Grants permissions to modify the SSL setting.	write	instance *	-
dcs:job:get	Grants permission to obtain the pre-check result.	read	-	-
dcs:task:list	Grants permission to list background tasks.	list	-	-
dcs:task:delete	Grants permission to delete background tasks.	write	-	-

Each API of DCS usually supports one or more actions. **Table 5-182** lists the supported actions and dependencies.

Table 5-182 Actions and dependencies supported by DCS APIs

API	Action	Dependencies
GET /v2/{project_id}/instances	dcs:instance:list	-

API	Action	Dependencies
DELETE /v2/{project_id}/instances	dcs:instance:delete	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get
GET /v2/{project_id}/instances/{instance_id}	dcs:instance:get	-
DELETE /v2/{project_id}/instances/{instance_id}	dcs:instance:delete	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get
PUT /v2/{project_id}/instances/{instance_id}	dcs:instance:modify	• vpc:ports:get • vpc:ports:update
POST /v2/{project_id}/instances/{instance_id}/resize	dcs:instance:scale	• vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:subnets:get • vpc:securityGroupRules:get • vpc:securityGroups:get
POST /v2/{project_id}/instances/{instance_id}/resize/check-job	dcs:instance:scale	-
POST /v2/{project_id}/instances/{instance_id}/swap	dcs:instance:swap	-
PUT /v2/{project_id}/instances/{instance_id}/password	dcs:instance:modifyAuthInfo	-

API	Action	Dependencies
POST /v2/{project_id}/instances/{instance_id}/password/reset	dcs:instance:modifyAuthInfo	-
GET /v2/{project_id}/instances/status	dcs:instance:list	-
PUT /v2/{project_id}/instances/status	dcs:instance:modifyStatus	-
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:getConfiguration	-
PUT /v2/{project_id}/instances/{instance_id}/configs	dcs:instance:modifyConfiguration	-

API	Action	Dependencies
PUT /v2/{project_id}/instances/{instance_id}/async-configs	dcs:instance:modifyConfiguration	-
DELETE /v2/{project_id}/instances/{instance_id}/backups/{backup_id}	dcs:instance:deleteDataBackupFile	-
POST /v2/{project_id}/instances/{instance_id}/restores	dcs:instance:restoreData	-
GET /v2/{project_id}/instances/{instance_id}/restores	dcs:instance:getDataRestoreLog	-
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:getDataBackupLog	-
POST /v2/{project_id}/migration-task	dcs:migrationTask:create	-
GET /v2/{project_id}/migration-tasks	dcs:migrationTask:list	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
GET /v2/{project_id}/instances/{instance_id}/bigkey-tasks	dcs:instance:listBigKey	-
PUT /v2/{project_id}/instances/{instance_id}/bigkey/autoscan	dcs:instance:updateBigKeyAutoScanConfig	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
POST /v2/{project_id}/instances/{instance_id}/redislog	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/redislog/{id}/links	dcs:redisLog:get	-
POST /v2/{project_id}/instances/{instance_id}/accounts	dcs:aclaccount:create	-
GET /v2/{project_id}/instances/{instance_id}/accounts	dcs:aclaccount:list	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/password/modify	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/password/reset	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}	dcs:aclaccount:modify	-
PUT /v2/{project_id}/instances/{instance_id}/accounts/{account_id}/role	dcs:aclaccount:modify	-

API	Action	Dependencies
DELETE /v2/{project_id}/instances/{instance_id}/accounts/{account_id}	dcs:aclaccount:delete	-
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}/dims/monitored-objects/{instance_id}	dcs:instance:get	-
GET /v2/{project_id}/dims/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	-

API	Action	Dependencies
GET /v2/{project_id}/diagnosis/{report_id}	dcs:instance:getDiagnosisTask	-
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	-

API	Action	Dependencies
PUT /v2/{project_id}/instances/{instance_id}/async-swap	dcs:instance:swap	-
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	-

API	Action	Dependencies
POST /v2/{project_id}/instances/{instance_id}/clients	dcs:clients:list	-
GET /v2/{project_id}/instances/{instance_id}/clients	dcs:clients:list	-
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	-

API	Action	Dependencies
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	-
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:getBackgroundTask	-
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	-
GET /v2/{project_id}/tasks	dcs:task:list	-

API	Action	Dependencies
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 SCP applies to. If you specify a resource type for any action in **Table 5-183**, 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 DCS.

Table 5-183 Resource types supported by DCS

Resource Type	URN
instance	dcs:*<region>*:*<account-id>*:instance:*<instance-id>*
migrationTask	dcs:*<region>*:*<account-id>*:migrationTask:*<task-id>*

Conditions

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, **dcs:**) only apply to operations of the DCS service. For details, see **Table 5-184**.
  - 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.

The following table lists the condition keys that you can define in SCPs for DCS. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-184 Service-specific condition keys supported by DCS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
dcs:backupEnabled	boolean	Single-valued	Controls the permission for enabling automated backup for DCS instances.

5.10.10.2 Cloud Service Engine (CSE)

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 CSE, 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 CSE, see **Conditions**.

The following table lists the actions that you can define in SCP statements for CSE.

Table 5-185 Supported Actions

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cse:config:upload	Assigning permissions to upload microservice configurations	write	-	g:EnterpriseProjectId
cse:config:download	Assigning permissions to download microservice configurations	write	-	g:EnterpriseProjectId
cse:namespace:list	Assigning permissions to view the namespace resource list	list	-	-
cse:namespace:get	Assigning permissions to view namespaces	read	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cse:namespace:create	Assigning permissions to create a namespace	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys
cse:namespace:update	Assigning permissions to modify namespace resources	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:namespace:delete	Assigning permissions to delete a namespace	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:policy:list	Assigning permissions to view the governance policy list	list	-	-
cse:policy:get	Assigning permissions to view governance policies	read	-	-
cse:policy:create	Assigning permissions to create a governance policy	write	-	-
cse:policy:update	Assigning permissions to modify governance policies	write	-	-
cse:policy:delete	Assigning permissions to delete a governance policy	write	-	-
cse:engine:get	Assigning permissions to view engines	read	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cse:engine:list	Assigning permissions to view the engine list	list	-	-
cse:engine:modify	Assigning permissions to change engine permissions	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:create	Assigning permissions to create an engine	write	-	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys
cse:engine:upgrade	Assigning permissions to upgrade engine permissions	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:delete	Assigning permissions to deleting an engine	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:tagResource	Assigning permissions to add engine tags	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:unTagResource	Assigning permissions to delete engine tags	write	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
cse:engine:listTags	Assigning permissions to view all engine tags of a project	list	-	-
cse:engine:listTagsForResource	Assigning permissions to view engine tags	list	engine	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cse:engine:listResourcesByTag	Assigning permissions to query the engine list by tag	list	-	g:TagKeys

Each API of CSE usually supports one or more actions. **Table 5-186** lists the actions and dependencies supported by CSE APIs.

Table 5-186 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:modify	-
GET /v2/{project_id}/enginemgr/engines/{engine_id}/jobs/{job_id}	cse:engine:get	-
GET /v2/{project_id}/enginemgr/engines	cse:engine:list	-
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	-

API	Action	Dependencies
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}/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	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/resize	cse:engine:modify	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/config	cse:engine:modify	-
PUT /v2/{project_id}/enginemgr/engines/{engine_id}/upgrade	cse:engine:upgrade	-
GET /v3/{project_id}/govern/governance/{kind}	cse:policy:list	-
POST /v3/{project_id}/govern/governance/{kind}	cse:policy:create	-
DELETE /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:delete	-
GET /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:get	-

API	Action	Dependencies
PUT /v3/{project_id}/govern/governance/{kind}/{policy_id}	cse:policy:update	-
GET /v3/{project_id}/govern/governance/display	cse:policy:list	-
DELETE /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:delete	-
PUT /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:update	-
GET /v3/{project_id}/govern/route-rule/microservices/{service_name}	cse:policy:get	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-187**, 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 CSE.

Table 5-187 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 SCPs.

It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.10.3 API Gateway (APIG)

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 IAM custom identity policies and 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 APIG, 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 APIG, see **Conditions**.

The following table lists the actions that you can define in SCP statements for APIG.

Table 5-188 Actions supported by APIG

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:acl:list	Grants permissions to query access control policies.	list	instance *	g:ResourceTag/<tag-key>	apig:acls:list
apig:acl:create	Grants permissions to create an access control policy.	write	instance *	g:ResourceTag/<tag-key>	apig:acls:create
apig:acl:batchDelete	Grants permissions to delete access control policies in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:acls:delete
apig:acl:delete	Grants permissions to delete an access control policy.	write	instance *	g:ResourceTag/<tag-key>	apig:acls:delete
apig:acl:get	Grants permissions to query access control policy details.	read	instance *	g:ResourceTag/<tag-key>	apig:acls:get
apig:acl:update	Grants permissions to modify an access control policy.	write	instance *	g:ResourceTag/<tag-key>	apig:acls:update
apig:api:bindAcl	Grants permissions to bind APIs with access control policies.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindAcls

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:api:batchUnbindAcl	Grants permissions to unbind access control policies from APIs in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindAcls
apig:api:unbindAcl	Grants permissions to unbind access control policies from APIs.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindAcls
apig:api:listBoundAcl	Grants permissions to query access control policies bound to a specified API.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedAcls
apig:acl:listBoundApi	Grants permissions to query APIs bound to a specified access control policy.	list	instance *	g:ResourceTag/<tag-key>	apig:acls:listBindedApis
apig:acl:listUnboundApi	Grants permissions to query APIs that are not bound to a specified access control policy.	list	instance *	g:ResourceTag/<tag-key>	apig:acls:listUnbindedApis
apig:api:bindRequestThrottling	Grants permissions to bind APIs with request throttling policies.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindThrottles

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:api:batchUnbindRequestThrottling	Grants permissions to unbind request throttling policies from APIs in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindThrottles
apig:api:unbindRequestThrottling	Grants permissions to unbind request throttling policies from APIs.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindThrottles
apig:requestThrottling:listBoundApi	Grants permissions to query APIs bound to a specified request throttling policy.	list	instance *	g:ResourceTag/<tag-key>	apig:throttles:listBindedApis
apig:api:listBoundRequestThrottling	Grants permissions to query request throttling policies bound to a specified API.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedThrottles
apig:requestThrottling:listUnboundApi	Grants permissions to query APIs that are not bound to a specified request throttling policy.	list	instance *	g:ResourceTag/<tag-key>	apig:throttles:listUnbindedApis

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:apiGroup:list	Grants permissions to query API groups.	list	instance *	g:ResourceTag/<tag-key>	apig:groups:list
apig:apiGroup:create	Grants permissions to create an API group.	write	instance *	g:ResourceTag/<tag-key>	apig:groups:create
apig:apiGroup:delete	Grants permissions to delete an API group.	write	instance *	g:ResourceTag/<tag-key>	apig:groups:delete
apig:apiGroup:get	Grants permissions to query API group details.	read	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:apiGroup:update	Grants permissions to modify an API group.	write	instance *	g:ResourceTag/<tag-key>	apig:groups:update
apig:apiGroup:checkApiGroupNameExistOrNot	Grants permissions to check whether the API group name exists.	read	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:api:list	Grants permissions to query APIs.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:list
apig:api:create	Grants permissions to create an API.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:create
apig:api:delete	Grants permissions to delete an API.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:delete

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:api:get	Grants permissions to query API details.	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:update	Grants permissions to modify an API.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:update
apig:api:onlineOrOffline	Grants permissions to publish or take an API offline.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:publish
apig:api:batchDelete	Grants permissions to delete APIs in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:delete
apig:api:checkApiPathOrApiNameExistOrNot	Grants permissions to verify the API definition.	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:debug	Grants permissions to debug an API.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:debug
apig:api:batchOnlineOrOffline	Grants permissions to publish or take APIs offline in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:publish
apig:api:listHistoryVersion	Grants permissions to query historical API versions.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:switchVersion	Grants permissions to switch the API version.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:publish

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:api:getRuntimeDefinition	Grants permissions to query the API runtime definition.	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:api:deleteHistoryVersion	Grants permissions to take an API offline based on the version ID.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:offline
apig:api:getHistoryVersion	Grants permissions to query version details.	read	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:app:list	Grants permissions to query apps.	list	instance *	g:ResourceTag/<tag-key>	apig:apps:list
apig:app:create	Grants permissions to create an app.	write	instance *	g:ResourceTag/<tag-key>	apig:apps:create
apig:app:delete	Grants permissions to delete an app.	write	instance *	g:ResourceTag/<tag-key>	apig:apps:delete
apig:app:get	Grants permissions to query app details.	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:update	Grants permissions to modify app information.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:update
apig:app:listAppCode	Grants permissions to query AppCodes.	list	instance *	g:ResourceTag/<tag-key>	apig:appCodes:list

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:app:createAppCode	Grants permissions to create an AppCode.	write	instance *	g:ResourceTag/<tag-key>	apig:appCodes:create
apig:app:generateAppCode	Grants permissions to automatically generate AppCodes.	write	instance *	g:ResourceTag/<tag-key>	apig:appCodes:update
apig:app:deleteAppCode	Grants permissions to delete an AppCode.	write	instance *	g:ResourceTag/<tag-key>	apig:appCodes:delete
apig:app:getAppCode	Grants permissions to query AppCode details.	read	instance *	g:ResourceTag/<tag-key>	apig:appCodes:get
apig:app:resetSecret	Grants permissions to reset the AppSecret.	write	instance *	g:ResourceTag/<tag-key>	apig:apps:update
apig:app:validate	Grants permissions to check whether a specified app exists.	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:getBoundQuota	Grants permissions to query the credential quota policies associated with a specified app.	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:bindApi	Grants permissions to bind APIs with apps.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:grantAppAccess

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:app:unbindApi	Grants permissions to unbind APIs from apps.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:relieveAppAccess
apig:app:listBoundApi	Grants permissions to query APIs bound to a specified app.	list	instance *	g:ResourceTag/<tag-key>	apig:apps:listBindedApis
apig:api:listBoundApp	Grants permissions to query apps bound to a specified API.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedApps
apig:app:listUnboundApi	Grants permissions to query APIs not bound to a specified app.	list	instance *	g:ResourceTag/<tag-key>	apig:apps:listUnbindedApis
apig:api:export	Grants permissions to export APIs.	read	instance *	g:ResourceTag/<tag-key>	apig:apis:export
apig:api:import	Grants permissions to import APIs.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:import
apig:asyncTask:get	Grants permission to query the result of an asynchronous task.	read	instance *	g:ResourceTag/<tag-key>	apig:apis:export
apig:certificate:list	Grants permissions to query SSL certificates.	list	instance	g:ResourceTag/<tag-key>	-

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:certificate:create	Grants permissions to create an SSL certificate.	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:delete	Grants permissions to delete an SSL certificate.	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:get	Grants permissions to query SSL certificate details.	read	instance	g:ResourceTag/<tag-key>	-
apig:certificate:update	Grants permissions to modify an SSL certificate.	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:listBoundDomain	Grants permissions to query domain names bound to a specified SSL certificate.	list	instance	g:ResourceTag/<tag-key>	-
apig:certificate:batchBindDomain	Grants permissions to bind a domain name to an SSL certificate.	write	instance	g:ResourceTag/<tag-key>	-
apig:certificate:batchUnbindDomain	Grants permissions to unbind domain names from a specified SSL certificate.	write	instance	g:ResourceTag/<tag-key>	-

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:apiGroup:batchBindCertificateToDomain	Grants permissions to bind an SSL certificate to a domain name.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:bindCertificate
apig:apiGroup:batchUnbindCertificateFromDomain	Grants permissions to unbind certificates from a specified domain name.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:unbindCertificate
apig:loadBalanceChannel:list	Grants permissions to query the load balance channels.	list	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:list
apig:loadBalanceChannel:create	Grants permissions to create a load balance channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:create
apig:loadBalanceChannel:delete	Grants permissions to delete a load balance channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:delete
apig:loadBalanceChannel:get	Grants permissions to query load balance channel details.	read	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get
apig:loadBalanceChannel:update	Grants permissions to update a load balance channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:update

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:loadBalanceChannel:updateHealthCheckConfig	Grants permissions to modify the health check configuration of a load balance channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:update
apig:loadBalanceChannel:listServerGroup	Grants permissions to query the backend server groups of a specified load balance channel.	list	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get
apig:loadBalanceChannel:createServerGroup	Grants permissions to add or update backend server groups of a specified VPC channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:addOrUpdateMemberGroups
apig:loadBalanceChannel:deleteServerGroup	Grants permissions to delete the backend server groups of a specified VPC channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:deleteMemberGroup
apig:loadBalanceChannel:getServerGroup	Grants permissions to query details about the backend server group of a specified VPC channel.	read	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:loadBalanceChannel:updateServerGroup	Grants permissions to update the backend server groups of a specified VPC channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:updateMemberGroup
apig:loadBalanceChannel:listBackendServerAddress	Grants permissions to query the backend instances of a specified load balance channel.	list	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:get
apig:loadBalanceChannel:createBackendServerAddress	Grants permissions to add or update backend instances of a specified load balance channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:addInstance
apig:loadBalanceChannel:updateBackendServerAddress	Grants permissions to update backend instances of a specified load balance channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:addInstance
apig:loadBalanceChannel:deleteBackendServerAddress	Grants permissions to delete backend instances of a specified load balance channel.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:deleteInstance

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:loadBalanceChannel:batchDisableBackendServerAddress	Grants permissions to disable backend servers in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:batchDisableInstance
apig:loadBalanceChannel:batchEnableBackendServerAddress	Grants permissions to enable backend servers in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:vpcChannels:batchEnableInstance
apig:instance:listTag	Grants permissions to query tags.	list	instance *	g:ResourceTag/<tag-key>	apig:tags:list
apig:api:listUnboundPlugin	Grants permissions to query plug-ins that can be bound to a specified API.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedPlugins
apig:api:listBoundPlugin	Grants permissions to query plug-ins bound to a specified API.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedPlugins
apig:api:bindPlugin	Grants permissions to bind a plug-in to an API.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindPlugins
apig:api:unbindPlugin	Grants permissions to unbind plug-ins from a specified API.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindPlugins

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:plugin:list	Grants permissions to query plug-ins.	list	instance *	g:ResourceTag/<tag-key>	apig:plugins:list
apig:plugin:create	Grants permission to create extensions.	write	instance *	g:ResourceTag/<tag-key>	apig:plugins:create
apig:plugin:delete	Grants permission to delete extensions.	write	instance *	g:ResourceTag/<tag-key>	apig:plugins:delete
apig:plugin:get	Grants permissions to query plug-in details.	read	instance *	g:ResourceTag/<tag-key>	apig:plugins:get
apig:plugin:update	Grants permissions to modify a plug-in.	write	instance *	g:ResourceTag/<tag-key>	apig:plugins:update
apig:plugin:bindApi	Grants permissions to bind an API to a plug-in.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindPlugins
apig:plugin:listUnbindApi	Grants permissions to query APIs that can be bound to a specified plug-in.	list	instance *	g:ResourceTag/<tag-key>	apig:plugins:listUnbindedApis
apig:plugin:listBoundApi	Grants permissions to query APIs bound to a specified plug-in.	list	instance *	g:ResourceTag/<tag-key>	apig:plugins:listBindedApis

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:plugin:unbindApi	Grants permissions to unbind APIs from a specified plug-in.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindPlugins
apig:apiGroup:listGatewayResponse	Grants permissions to query the responses of a specified API group.	list	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:list
apig:apiGroup:createGatewayResponse	Grants permissions to create a group response.	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:create
apig:apiGroup:deleteGatewayResponse	Grants permissions to delete a group response.	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:delete
apig:apiGroup:getGatewayResponse	Grants permissions to query group response details.	read	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:get
apig:apiGroup:updateGatewayResponse	Grants permissions to modify a group response.	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:updat
apig:apiGroup:deleteGatewayResponseType	Grants permissions to delete the response of an error type defined for an API group.	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:update

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:apiGroup:getGatewayResponseType	Grants permissions to query the response of an error type defined for an API group.	read	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:get
apig:apiGroup:updateGatewayResponseType	Grants permissions to modify the response of an error type defined for an API group.	write	instance *	g:ResourceTag/<tag-key>	apig:gatewayResponses:update
apig:instance:listApiOutline	Grants permissions to query API quantities.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:instance:listAppOutline	Grants permissions to query app quantities.	list	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:instance:listApiGroupOutline	Grants permissions to query API group quantities.	list	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:environmentVariable:list	Grants permissions to query environment variables.	list	instance *	g:ResourceTag/<tag-key>	apig:variables:list
apig:environmentVariable:create	Grants permissions to create an environment variable.	write	instance *	g:ResourceTag/<tag-key>	apig:variables:create

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:environmentVariable:delete	Grants permissions to delete an environment variable.	write	instance *	g:ResourceTag/<tag-key>	apig:variables:delete
apig:environmentVariable:get	Grants permissions to query environment variable details.	read	instance *	g:ResourceTag/<tag-key>	apig:variables:get
apig:environmentVariable:update	Grants permissions to modify an environment variable.	write	instance *	g:ResourceTag/<tag-key>	apig:variables:update
apig:environment:list	Grants permissions to query environments.	list	instance *	g:ResourceTag/<tag-key>	apig:envs:list
apig:environment:create	Grants permissions to create an environment.	write	instance *	g:ResourceTag/<tag-key>	apig:envs:create
apig:environment:delete	Grants permissions to delete an environment.	write	instance *	g:ResourceTag/<tag-key>	apig:envs:delete
apig:environment:update	Grants permissions to modify an environment.	write	instance *	g:ResourceTag/<tag-key>	apig:envs:update
apig:instance:listMetricData	Grants permissions to query metric data of a specified gateway.	list	instance *	g:ResourceTag/<tag-key>	apig:metricData:get

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:instance:listApiMonitoring	Grants permissions to query API calls within a specific period.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:get
apig:instance:listApiGroupMonitoring	Grants permissions to query API calls under an API group in the last one hour.	list	instance *	g:ResourceTag/<tag-key>	apig:groups:get
apig:requestThrottling:list	Grants permissions to query request throttling policies.	list	instance *	g:ResourceTag/<tag-key>	apig:throttles:list
apig:requestThrottling:create	Grants permissions to create a request throttling policy.	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:create
apig:requestThrottling:delete	Grants permissions to delete a request throttling policy.	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:delete
apig:requestThrottling:get	Grants permissions to query request throttling policy details.	read	instance *	g:ResourceTag/<tag-key>	apig:throttles:get

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:requestThrottling:update	Grants permissions to modify a request throttling policy.	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:update
apig:requestThrottling:batchDelete	Grants permissions to delete request throttling policies in batches.	write	instance *	g:ResourceTag/<tag-key>	apig:throttles:delete
apig:api:bindSignatureKey	Grants permissions to bind signature keys to APIs.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:bindSigns
apig:api:unbindSignatureKey	Grants permissions to unbind signature keys from APIs.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:unbindSigns
apig:signatureKey:listBoundApi	Grants permissions to query APIs bound to a specified signature key.	list	instance *	g:ResourceTag/<tag-key>	apig:signs:listBindedApis
apig:api:listBoundSignatureKey	Grants permissions to query signature keys bound to a specified API.	list	instance *	g:ResourceTag/<tag-key>	apig:apis:listBindedSigns
apig:signatureKey:listUnboundApi	Grants permissions to query APIs not bound to a specified signature key.	list	instance *	g:ResourceTag/<tag-key>	apig:signs:listUnbindedApis

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:signatureKey:list	Grants permissions to query signature keys.	list	instance *	g:ResourceTag/<tag-key>	apig:signs:list
apig:signatureKey:create	Grants permissions to create a signature key.	write	instance *	g:ResourceTag/<tag-key>	apig:signs:create
apig:signatureKey:delete	Grants permissions to delete a signature key.	write	instance *	g:ResourceTag/<tag-key>	apig:signs:delete
apig:signatureKey:update	Grants permissions to modify a signature key.	write	instance *	g:ResourceTag/<tag-key>	apig:signs:update
apig:requestThrottling:listSpecial	Grants permissions to query excluded request throttling configurations.	list	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:get
apig:requestThrottling:createSpecial	Grants permissions to create an excluded request throttling configuration.	write	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:create
apig:requestThrottling:deleteSpecial	Grants permissions to delete an excluded request throttling configuration.	write	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:delete

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:requestThrottling:updateSpecial	Grants permissions to modify an excluded configuration of a specified request throttling policy.	write	instance *	g:ResourceTag/<tag-key>	apig:specialThrottles:update
apig:instance:listSingleInstanceTag	Grants permissions to query tags of a specified gateway.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instanceTags:list
apig:instance:batchCreateOrDeleteTag	Grants permissions to add or delete gateway tags in batches.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instanceTags:create
			-	• g:RequestTag/<tag-key> • g:TagKeys	
apig::listTag	Grants permissions to query all gateway tags in the project.	list	-	-	apig:instanceTags:list
apig:instance:getNumByTags	Grants permissions to query the number of gateways by tag.	read	instance *	-	-
			-	g:TagKeys	
apig:instance:listByTags	Grants permissions to query gateways by tag.	list	instance *	-	-
			-	g:TagKeys	

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:instance:list	Grants permissions to query dedicated gateways.	list	-	-	apig:instances:list
apig:instance:create	Grants permissions to create a dedicated gateway.	write	-	• g:RequestTag/<tag-key> • g:TagKeys	apig:instances:create
apig:instance:delete	Grants permissions to delete a dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:delete
apig:instance:get	Grants permissions to query dedicated gateway details.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:get
apig:instance:update	Grants permissions to update a dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:unbindEip	Grants permissions to unbind an EIP from a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:bindOrChangeEip	Grants permissions to add or change EIPs of a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:instance:deleteOutboundEip	Grants permissions to disable public outbound access for a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:createOutboundEip	Grants permissions to enable public outbound access for a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:changeOutboundEipBandwidth	Grants permissions to modify the public outbound access bandwidth of a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:getCreateProgress	Grants permissions to query the creation progress of a specified dedicated gateway.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:instance:deleteIngressEip	Grants permissions to disable the public inbound access for a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:createIngressEip	Grants permissions to enable the public inbound access for a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:changeIngressEipBindwidth	Grants permissions to update the public outbound access bandwidth of a specified dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:update
apig:instance:resize	Grants permissions to create a specification change order for a pay-per-use dedicated gateway.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:getRestriction	Grants permissions to query gateway constraint information.	read	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:instances:get

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:instance:listParameter	Grants permissions to query the gateway parameters.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:features:list
apig:instance:updateParameter	Grants permissions to edit the gateway parameters.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	apig:features:create
apig:instance:listFeature	Grants permissions to query features supported by a specified gateway.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:importMicroservice	Grants permissions to import microservices to a dedicated gateway.	write	instance *	g:ResourceTag/<tag-key>	apig:apis:import
apig:apiGroup:bindDomain	Grants permissions to bind independent domain names.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:create
apig:apiGroup:unbindDomain	Grants permissions to unbind independent domain names.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:delete
apig:apiGroup:updateDomainConfig	Grants permissions to modify an independent domain name.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:update

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:apiGroup:createAndBindCertificateToDomain	Grants permissions to create certificates and bind them to independent domain names.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:bindCertificate
apig:apiGroup:unbindAndDeleteCertificateFromDomain	Grants permissions to delete certificates and delete them from independent domain names.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:unbindCertificate
apig:apiGroup:getCertificateOfDomain	Grants permissions to query certificates of independent domain names.	read	instance *	g:ResourceTag/<tag-key>	apig:domains:getCertificate
apig:apiGroup:updateSLDomainSetting	Grants permissions to set accessibility of a debugging domain name.	write	instance *	g:ResourceTag/<tag-key>	apig:domains:updateSLDomainSetting
apig:customAuthorizer:list	Grants permissions to query custom authorizers.	list	instance *	g:ResourceTag/<tag-key>	apig:authorizers:list

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:customAuthorizer:create	Grants permissions to create a custom authorizer.	write	instance *	g:ResourceTag/<tag-key>	apig:authorizers:create
apig:customAuthorizer:delete	Grants permissions to delete a custom authorizer.	write	instance *	g:ResourceTag/<tag-key>	apig:authorizers:delete
apig:customAuthorizer:get	Grants permissions to query custom authorizer details.	read	instance *	g:ResourceTag/<tag-key>	apig:authorizers:get
apig:customAuthorizer:update	Grants permissions to modify a custom authorizer.	write	instance *	g:ResourceTag/<tag-key>	apig:authorizers:update
apig:instance:listVpcEndpoint	Grants permissions to query the VPC endpoint connections of a specified gateway.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:acceptOrRejectVpcEndpointConnection	Grants permissions to accept or reject VPC endpoint connections.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:instance:listVpcEndpointPermission	Grants permissions to query the whitelist records of a gateway's VPC endpoint service.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:batchAddVpcEndpointPermission	Grants permissions to add whitelist records of a gateway's VPC endpoint service in batches.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:batchDeleteVpcEndpointPermission	Grants permissions to delete whitelist records of a gateway's VPC endpoint service in batches.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:app:deleteAcl	Grants permissions to delete an access control rule of a credential.	write	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:app:getAcl	Grants permissions to query access control rules of a credential.	read	instance *	g:ResourceTag/<tag-key>	apig:apps:get

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:app:updateAcl	Grants permissions to set access control rules of credentials.	write	instance *	g:ResourceTag/<tag-key>	apig:apps:get
apig:clientQuota:list	Grants permissions to query credential quota policies.	list	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:create	Grants permissions to create a credential quota policy.	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:delete	Grants permissions to delete a credential quota policy.	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:get	Grants permissions to query credential quota policy details.	read	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:update	Grants permissions to modify a credential quota policy.	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:listBoundApp	Grants permissions to query the credentials bound to quota policies.	list	instance *	g:ResourceTag/<tag-key>	-

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:clientQuota:bindApp	Grants permissions to bind credential quotas with credentials.	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:unbindApp	Grants permissions to unbind credential quotas from credentials.	write	instance *	g:ResourceTag/<tag-key>	-
apig:clientQuota:listUnboundApp	Grants permissions to query credentials that can be bound to a specified credential quota.	list	instance *	g:ResourceTag/<tag-key>	-
apig:instance:listFeatureHistory	Grants permissions to query the feature history.	list	instance *	g:ResourceTag/<tag-key>	-
apig:instance:addCustomIngressPort	Grants permissions to add a custom inbound port.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:listCustomIngressPort	Grants permissions to query custom inbound ports.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

Action	Description.	Access Level	Resource Type (*: required)	Condition Key	Alias
apig:instance:deleteCustomIngressPort	Grants permissions to delete a custom inbound port.	write	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-
apig:instance:listCustomIngressPortDomain	Grants permissions to query domain names bound to a custom inbound port.	list	instance *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId	-

Each API of APIG usually supports one or more actions. **Table 5-189** lists the supported actions and dependencies.

Table 5-189 Actions and dependencies supported by APIG APIs

API	Action	Dependencies
GET /{project_id}/apigw/instances/{instance_id}/acls	apig:acl:list	apig:instance:get
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

API	Action	Dependencies
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	• apig:instance:get • apig:api:get • apig:acl:get
PUT /{project_id}/apigw/instances/{instance_id}/acl-bindings	apig:api:batchUnbindAcl	• apig:instance:get • apig:api:get • apig:acl:get
DELETE /{project_id}/apigw/instances/{instance_id}/acl-bindings/{acl_bindings_id}	apig:api:unbindAcl	• apig:instance:get • apig:api:get • apig:acl:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-acls	apig:api:listBoundAcl	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/binded-apis	apig:acl:listBoundApi	• apig:instance:get • apig:acl:get
GET /{project_id}/apigw/instances/{instance_id}/acl-bindings/unbinded-apis	apig:acl:listUnboundApi	• apig:instance:get • apig:acl:get
POST /{project_id}/apigw/instances/{instance_id}/throttle-bindings	apig:api:bindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get
PUT /{project_id}/apigw/instances/{instance_id}/throttle-bindings	apig:api:batchUnbindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get

API	Action	Dependencies
DELETE /{project_id}/apigw/instances/{instance_id}/throttle-bindings/{throttle_binding_id}	apig:api:unbindRequestThrottling	• apig:instance:get • apig:api:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-apis	apig:requestThrottling:listBoundApi	• apig:instance:get • apig:requestThrottling:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/binded-throttles	apig:api:listBoundRequest-Throttling	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/throttle-bindings/unbinded-apis	apig:requestThrottling:listUnboundApi	• apig:instance:get • apig:requestThrottling:get
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
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}	apig:apiGroup:update	apig:instance:get

API	Action	Dependencies
POST /{project_id}/apigw/instances/{instance_id}/api-groups/check	apig:apiGroup:checkApiGroupNameExistOrNot	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/apis	apig:api:list	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/apis	apig:api:create	• apig:instance:get • apig:apiGroup:get • apig:loadBalanceChannel:get • apig:customAuthorizer:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:delete	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:get	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}	apig:api:update	• apig:instance:get • apig:apiGroup:get • apig:loadBalanceChannel:get • apig:customAuthorizer:get • functiongraph:function:getFunctionConfig
POST /{project_id}/apigw/instances/{instance_id}/apis/action	apig:api:onlineOrOffline	• apig:instance:get • apig:apiGroup:get • apig:environment:list
-	apig:api:batchDelete	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/apis/check	apig:api:checkApiPathOrApiNameExistOrNot	• apig:instance:get • apig:apiGroup:get

API	Action	Dependencies
POST /{project_id}/apigw/instances/{instance_id}/apis/debug/{api_id}	apig:api:debug	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/apis/publish	apig:api:batchOnlineOrOffline	• apig:instance:get • apig:apiGroup:get • apig:environment:list
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	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/apis/runtime/{api_id}	apig:api:getRuntimeDefinition	• apig:instance:get • apig:environment:list
DELETE /{project_id}/apigw/instances/{instance_id}/apis/versions/{version_id}	apig:api:deleteHistoryVersion	• apig:instance:get • apig:apiGroup:get • apig:environment:list
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

API	Action	Dependencies
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	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:createAppCode	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes	apig:app:generateAppCode	• apig:instance:get • apig:app:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:app:deleteAppCode	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-codes/{app_code_id}	apig:app:getAppCode	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/secret/{app_id}	apig:app:resetSecret	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/validation/{app_id}	apig:app:validate	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/bound-quota	apig:app:getBoundQuota	• apig:instance:get • apig:app:get

API	Action	Dependencies
POST /{project_id}/apigw/instances/{instance_id}/app-auths	apig:app:bindApi	• apig:instance:get • apig:app:get • apig:api:get
DELETE /{project_id}/apigw/instances/{instance_id}/app-auths/{app_auth_id}	apig:app:unbindApi	• apig:instance:get • apig:app:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apis	apig:app:listBoundApi	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/binded-apps	apig:api:listBoundApp	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/app-auths/unbinded-apis	apig:app:listUnboundApi	• apig:instance:get • apig:app:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/export	apig:api:export	• apig:instance:get • apig:api:list • apig:api:get • apig:api:listBoundAcl • apig:acl:get • apig:api:listBoundRequestThrottling • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:api:listBoundPlugin • apig:plugin:get

API	Action	Dependencies
POST /{project_id}/apigw/instances/{instance_id}/openapi/async-export	apig:api:export	• apig:instance:get • apig:api:list • apig:api:get • apig:api:listBoundAcl • apig:acl:get • apig:api:listBoundRequestThrottling • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:api:listBoundPlugin • apig:plugin:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/import	apig:api:import	• apig:instance:get • apig:api:get • apig:acl:get • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:plugin:get
POST /{project_id}/apigw/instances/{instance_id}/openapi/async-import	apig:api:import	• apig:instance:get • apig:api:get • apig:acl:get • apig:requestThrottling:get • apig:apiGroup:get • apig:apiGroup:getGatewayResponse • apig:environment:list • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/async-tasks/{task_id}	apig:asyncTask:get	apig:instance:get

API	Action	Dependencies
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	• apig:certificate:get • apig:apiGroup:get
POST /{project_id}/apigw/certificates/{certificate_id}/domains/detach	apig:certificate:batchUnbindDomain	• apig:certificate:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/attach	apig:apiGroup:batchBindCertificateToDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificates/detach	apig:apiGroup:batchUnbindCertificateFromDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get

API	Action	Dependencies
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	• apig:instance:get • cce:cluster:getCluster • ecs:cloudServers:showServer • cce:cluster:generateClientCredential
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	• apig:instance:get • cce:cluster:getCluster • ecs:cloudServers:showServer • cce:cluster:generateClientCredential
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/health-config	apig:loadBalanceChannel:updateHealthCheckConfig	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups	apig:loadBalanceChannel:listServerGroup	• apig:instance:get • apig:loadBalanceChannel:get

API	Action	Dependencies
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups	apig:loadBalanceChannel:createServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:deleteServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:getServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/member-groups/{member_group_id}	apig:loadBalanceChannel:updateServerGroup	• apig:instance:get • apig:loadBalanceChannel:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:listBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:createBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get • ecs:cloudServers:showServer
PUT /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members	apig:loadBalanceChannel:updateBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get • ecs:cloudServers:showServer

API	Action	Dependencies
DELETE /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/{member_id}	apig:loadBalanceChannel:deleteBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-disable	apig:loadBalanceChannel:batchDisableBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-channels/{vpc_channel_id}/members/batch-enable	apig:loadBalanceChannel:batchEnableBackendServerAddress	• apig:instance:get • apig:loadBalanceChannel:get
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	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/attached-plugins	apig:api:listBoundPlugin	• apig:instance:get • apig:api:get
POST /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/attach	apig:api:bindPlugin	• apig:instance:get • apig:api:get • apig:plugin:get
PUT /{project_id}/apigw/instances/{instance_id}/apis/{api_id}/plugins/detach	apig:api:unbindPlugin	• apig:instance:get • apig:api:get • apig:plugin:get

API	Action	Dependencies
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	• apig:instance:get • apig:loadBalanceChannel:get • functiongraph:function:getFunctionConfig
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	• apig:instance:get • apig:loadBalanceChannel:get • functiongraph:function:getFunctionConfig
POST /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attach	apig:plugin:bindApi	• apig:instance:get • apig:api:get • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attachable-apis	apig:plugin:listUnbindApi	• apig:instance:get • apig:plugin:get
GET /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/attached-apis	apig:plugin:listBoundApi	• apig:instance:get • apig:plugin:get
PUT /{project_id}/apigw/instances/{instance_id}/plugins/{plugin_id}/detach	apig:plugin:unbindApi	• apig:instance:get • apig:api:get • apig:plugin:get

API	Action	Dependencies
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:apiGroup:listGatewayResponse	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses	apig:apiGroup:createGatewayResponse	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:deleteGatewayResponse	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:getGatewayResponse	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}	apig:apiGroup:updateGatewayResponse	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:deleteGatewayResponseType	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:getGatewayResponseType	• apig:instance:get • apig:apiGroup:get

API	Action	Dependencies
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/gateway-responses/{response_id}/{response_type}	apig:apiGroup:updateGatewayResponseType	• apig:instance:get • apig:apiGroup:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/apis	apig:instance:listApiOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/apps	apig:instance:listAppOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/resources/outline/groups	apig:instance:listApiGroupOutline	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/env-variables	apig:environmentVariable:list	• apig:instance:get • apig:apiGroup:get • apig:environment:list
POST /{project_id}/apigw/instances/{instance_id}/env-variables	apig:environmentVariable:create	• apig:instance:get • apig:apiGroup:get • apig:environment:list
DELETE /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:delete	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:get	• apig:instance:get • apig:apiGroup:get • apig:environment:list

API	Action	Dependencies
PUT /{project_id}/apigw/instances/{instance_id}/env-variables/{env_variable_id}	apig:environmentVariable:update	• apig:instance:get • apig:apiGroup:get • apig:environment:list
GET /{project_id}/apigw/instances/{instance_id}/envs	apig:environment:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/envs	apig:environment:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/envs/{env_id}	apig:environment:delete	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/envs/{env_id}	apig:environment:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/metric-data	apig:instance:listMetricData	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/statistics/api/latest	apig:instance:listApiMonitoring	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/statistics/group/latest	apig:instance:listApiGroupMonitoring	apig:instance:get
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

API	Action	Dependencies
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
-	apig:requestThrottling:batchDelete	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/sign-bindings	apig:api:bindSignatureKey	• apig:instance:get • apig:api:get • apig:signatureKey:list
DELETE /{project_id}/apigw/instances/{instance_id}/sign-bindings/{sign_bindings_id}	apig:api:unbindSignatureKey	• apig:instance:get • apig:api:get • apig:signatureKey:list
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-apis	apig:signatureKey:listBoundApi	• apig:instance:get • apig:signatureKey:list
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/binded-signs	apig:api:listBoundSignatureKey	• apig:instance:get • apig:api:get
GET /{project_id}/apigw/instances/{instance_id}/sign-bindings/unbinded-apis	apig:signatureKey:listUnboundApi	• apig:instance:get • apig:signatureKey:list

API	Action	Dependencies
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	• apig:instance:get • apig:requestThrottling:get
POST /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials	apig:requestThrottling:createSpecial	• apig:instance:get • apig:requestThrottling:get
DELETE /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:requestThrottling:deleteSpecial	• apig:instance:get • apig:requestThrottling:get
PUT /{project_id}/apigw/instances/{instance_id}/throttles/{throttle_id}/throttle-specials/{strategy_id}	apig:requestThrottling:updateSpecial	• apig:instance:get • apig:requestThrottling:get

API	Action	Dependencies
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	• vpc:securityGroups:get • vpc:ports:create • vpc:ports:update • eip:publicIps:get • eip:publicIps:update • eps:enterpriseProjects:list
DELETE /{project_id}/apigw/instances/{instance_id}	apig:instance:delete	• eip:publicIps:get • eip:publicIps:update • vpc:ports:delete
GET /{project_id}/apigw/instances/{instance_id}	apig:instance:get	-
PUT /{project_id}/apigw/instances/{instance_id}	apig:instance:update	• vpc:securityGroups:get • vpc:ports:update
DELETE /{project_id}/apigw/instances/{instance_id}/eip	apig:instance:unbindEip	• apig:instance:get • eip:publicIps:update
PUT /{project_id}/apigw/instances/{instance_id}/eip	apig:instance:bindOrChangeEip	• apig:instance:get • eip:publicIps:update

API	Action	Dependencies
DELETE /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:deleteOutboundEip	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:createOutboundEip	• apig:instance:get • vpc:ports:get
PUT /{project_id}/apigw/instances/{instance_id}/nat-eip	apig:instance:changeOutboundEipBandwidth	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/progress	apig:instance:getCreateProgress	-
DELETE /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:deleteIngressEip	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:createIngressEip	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/ingress-eip	apig:instance:changeIngressEipBindwidth	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/postpaid-resize	apig:instance:resize	apig:instance:get
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

API	Action	Dependencies
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	• apig:instance:get • apig:api:create • apig:apiGroup:get • apig:apiGroup:create • apig:loadBalanceChannel:get • apig:loadBalanceChannel:create • cce:cluster:getCluster • cce:cluster:generateClientCredential
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains	apig:apiGroup:bindDomain	• apig:instance:get • apig:apiGroup:get
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}	apig:apiGroup:unbindDomain	• apig:instance:get • apig:apiGroup:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}	apig:apiGroup:updateDomainConfig	• apig:instance:get • apig:apiGroup:get
POST /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate	apig:apiGroup:createAndBindCertificateToDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get

API	Action	Dependencies
DELETE /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}	apig:apiGroup:unbindAndDeleteCertificateFromDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
GET /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/domains/{domain_id}/certificate/{certificate_id}	apig:apiGroup:getCertificateOfDomain	• apig:instance:get • apig:apiGroup:get • apig:certificate:get
PUT /{project_id}/apigw/instances/{instance_id}/api-groups/{group_id}/sl-domain-access-settings	apig:apiGroup:updateSLDomainSetting	• apig:instance:get • apig:apiGroup:get
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	• apig:instance:get • functiongraph:function:getFunctionConfig
DELETE /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:get	apig:instance:get

API	Action	Dependencies
PUT /{project_id}/apigw/instances/{instance_id}/authorizers/{authorizer_id}	apig:customAuthorizer:update	• apig:instance:get • functiongraph:function:getFunctionConfig
GET /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections	apig:instance:listVpcEndpoint	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/connections/action	apig:instance:acceptOrRejectVpcEndpointConnection	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions	apig:instance:listVpcEndpointPermission	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-add	apig:instance:batchAddVpcEndpointPermission	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/vpc-endpoint/permissions/batch-delete	apig:instance:batchDeleteVpcEndpointPermission	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:deleteAcl	• apig:instance:get • apig:app:get
GET /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:getAcl	• apig:instance:get • apig:app:get
PUT /{project_id}/apigw/instances/{instance_id}/apps/{app_id}/app-acl	apig:app:updateAcl	• apig:instance:get • apig:app:get

API	Action	Dependencies
GET /{project_id}/apigw/instances/{instance_id}/app-quotas	apig:clientQuota:list	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/app-quotas	apig:clientQuota:create	apig:instance:get
DELETE /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:delete	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:get	apig:instance:get
PUT /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}	apig:clientQuota:update	apig:instance:get
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps	apig:clientQuota:listBoundApp	apig:instance:get
POST /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/binding-apps	apig:clientQuota:bindApp	• apig:instance:get • apig:clientQuota:get
DELETE /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bound-apps/{app_id}	apig:clientQuota:unbindApp	• apig:instance:get • apig:app:get • apig:clientQuota:get

API	Action	Dependencies
GET /{project_id}/apigw/instances/{instance_id}/app-quotas/{app_quota_id}/bindable-apps	apig:clientQuota:listUnboundApp	• apig:instance:get • apig:clientQuota:get
-	apig:instance:listFeatureHistory	• apig:instance:get • apig:instance:listFeature
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	• apig:instance:get • apig:instance:listCustomIngressPort
GET /{project_id}/apigw/instances/{instance_id}/custom-ingress-ports/{ingress_port_id}/domains	apig:instance:listCustomIngressPortDomain	• apig:instance:get • apig:apiGroup:get • apig:instance:listCustomIngressPort

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-190**, 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 APIG.

Table 5-190 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 SCPs. It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.11 Developer Services

5.10.11.1 ServiceStage

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 IAM custom identity policies and 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 identity policy 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 ServiceStage, 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 ServiceStage, see **Conditions**.

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

Table 5-191 Actions supported by ServiceStage

Action	Description	Access Level	Resource Type	Condition Key
servicestage:app:getApplication	Querying an application	read	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
servicestage:app:createApplication	Creating an application	write	app	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:app:modifyApplication	Updating an application	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key> • g:RequestTag/<tag-key> • g:TagKeys
servicestage:app:deleteApplication	Deleting an application	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
servicestage:app:listApplication	Querying the application list	list	-	-
servicestage:app:getConfiguration	Querying application configuration	read	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type	Condition Key
servicestage:app:deleteConfiguration	Deleting application configuration	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
servicestage:app:modifyConfiguration	Updating application configuration	write	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
servicestage:app:getComponent	Querying an application component	read	app	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
servicestage:app:createComponent	Creating an application component	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:app:modifyComponent	Updating an application component	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:app:deleteComponent	Deleting an application component	write	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:app:listComponent	Querying the application component list	list	-	-
servicestage:environment:create	Creating an environment	write	environment	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:environment:get	Querying an environment	read	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:environment:list	Querying the environment list	list	-	-

Action	Description	Access Level	Resource Type	Condition Key
servicestage:environment:modify	Updating an environment	write	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:environment:delete	Deleting an environment	write	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:environment:tag	(TMS users) Creating an environment tag	tagging	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:app:tag	(TMS users) Creating an application tag	tagging	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:environment:listResourcesByTag	(TMS users) Querying environments by tag	read	environment	• g:RequestTag/<tag-key> • g:TagKeys
servicestage:app:listResourcesByTag	(TMS users) Querying applications by tag	read	app	• g:RequestTag/<tag-key> • g:TagKeys
servicestage:environment:unTagResource	(TMS users) Deleting an environment tag	tagging	environment	• g:ResourceTag/<tag-key> • g:RequestTag/<tag-key> • g:EnterpriseProjectId • g:TagKeys

Action	Description	Access Level	Resource Type	Condition Key
servicestage:app:unTagResource	(TMS users) Deleting an application tag	tagging	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
servicestage:environment:listTags	(TMS users) Querying the environment tag list	read	-	-
servicestage:app:listTags	(TMS users) Querying the application tag list	read	-	-
servicestage:pipeline:get	Querying a pipeline	read	pipeline	-
servicestage:pipeline:create	Creating a pipeline	write	pipeline	-
servicestage:pipeline:modify	Updating a pipeline	write	pipeline	-
servicestage:pipeline:delete	Deleting a pipeline	write	pipeline	-
servicestage:pipeline:list	Querying the pipeline list	list	-	-
servicestage:assembling:runtimeList	Querying the technology stack list	read	-	-
servicestage:assembling:getInfo	Querying a build task	list	-	-
servicestage:assembling:create	Creating a build task	write	assembling	-
servicestage:assembling:modify	Updating a build task	write	assembling	-

Action	Description	Access Level	Resource Type	Condition Key
servicestage:assembling:delete	Deleting a build task	write	assembling	-
servicestage:assembling:list	Querying the build task list	list	-	-
servicestage:repositoryAuth:list	Obtaining the repository authorization list	list	-	-
servicestage:repositoryAuth:get	Obtaining repository authorization	read	repositoryAuth	-
servicestage:repositoryAuth:create	Creating repository authorization	write	repositoryAuth	-
servicestage:repositoryAuth:delete	Deleting repository authorization	write	repositoryAuth	-
servicestage:environment:listTagsForResource	(EPS users) Querying the environment tag list	read	environment	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
servicestage:app:listTagsForResource	(EPS users) Querying the application tag list	read	app	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Each API of ServiceStage usually supports one or more actions. **Table 5-192** lists the actions and dependencies supported by ServiceStage APIs.

Table 5-192 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	-

API	Action	Dependencies
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	-

API	Action	Dependencies
DELETE /v2/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:deleteConfiguration	-
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 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 servicestage:assembling:create

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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/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	-
GET /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:getConfiguration	-
PUT /v3/{project_id}/cas/applications/{application_id}/configuration	servicestage:app:modifyConfiguration	-

API	Action	Dependencies
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 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	-

API	Action	Dependencies
GET /v3/{project_id}/cas/runtimestacks	servicestage:app:listApplication	-
GET /v1/{project_id}/git/auths	servicestage:repositoryAuth:list	-
GET /v1/{project_id}/git/auths/{repo_type}/redirect	servicestage:repositoryAuth:get	-
POST /v1/{project_id}/git/auths/{repo_type}/oauth	servicestage:repositoryAuth:create	-
POST /v1/{project_id}/git/auths/{repo_type}/personal	servicestage:repositoryAuth:create	-
POST /v1/{project_id}/git/auths/{repo_type}/password	servicestage:repositoryAuth:create	-
DELETE /v1/{project_id}/git/auths/{name}	servicestage:repositoryAuth:delete	-
GET /v2/{project_id}/servicestage-environment/{environment_id}/tags	servicestage:environment:listTagsForResource	-
GET /v2/{project_id}/servicestage-application/{app_id}/tags	servicestage:app:listTagsForResource	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-193**, 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 ServiceStage.

Table 5-193 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>

Conditions

ServiceStage 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.

5.10.11.2 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 5-194 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	-	-
codearts:cloudbuild:viewUsage	Grants permission to check CodeArts Build resource usage on the console.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codearts:codecheck:viewUsage	Grants permission to check CodeArts Check resource usage on the console.	read	-	-
codearts:cloudtest: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	-	-
codearts:cloudide:viewUsage	Grants permission to check CodeArts IDE resource usage on the console.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-	-
codearts:cloudbuild:subscribeService	Grants permission to subscribe to CodeArts Build in pay-per-use mode on the console.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codearts:codecheck:subscribeService	Grants permission to subscribe to CodeArts Check in pay-per-use mode on the console.	write	-	-
codearts:cloudtest: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	-	-
codearts:package:subscribeService	Grants permission to subscribe to a pay-per-use package on the console.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-	-
codearts:cloudbuild:unsubscribeService	Grants permission to unsubscribe from CodeArts Build in pay-per-use mode on the console.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codearts:codecheck:unsubscribeService	Grants permission to unsubscribe from CodeArts Check in pay-per-use mode on the console.	write	-	-
codearts:cloudtest: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	-	-
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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-	-
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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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:cloudtest: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	-	-
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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-	-
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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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	-	-
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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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.

5.10.11.3 CodeArts Pipeline

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 edit 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 CodeArts Pipeline, 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 of an action is empty (-), the condition key takes effect for all resources.
  - If this column does not have any values (-), the action does not support any condition keys.

  For details about the condition keys defined by CodeArts Pipeline, see **Condition**.

The following table lists the actions that you can define in SCP statements for CodeArts Pipeline.

Table 5-195 Actions supported by CodeArts Pipeline

Item	Description	Access Level	Resource Type (*: required)	Condition Key
codeartspipeline:pipelinetemplate:create	Grants permission to create pipeline templates.	write	-	-
codeartspipeline:pipelinetemplate:update	Grants permission to update pipeline templates.	write	-	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
codeartspipeline:pipelinetemplate:delete	Grants permission to delete pipeline templates.	write	-	-
codeartspipeline:pipelinetemplate:get	Grants permission to view pipeline templates.	read	-	-
codeartspipeline:pipelinetemplate:list	Grants permission to view the pipeline template list.	list	-	-
codeartspipeline:rule:create	Grants permission to create rules.	write	-	-
codeartspipeline:rule:update	Grants permission to update rules.	write	-	-
codeartspipeline:rule:delete	Grants permission to delete rules.	write	-	-
codeartspipeline:rule:get	Grants permission to view rules.	read	-	-
codeartspipeline:rule:list	Grants permission to view the rule list.	list	-	-
codeartspipeline:strategy:create	Grants permission to create policies.	write	-	-
codeartspipeline:strategy:update	Grants permission to update policies.	write	-	-

Item	Description	Access Level	Resource Type (*: required)	Condition Key
codeartspipeline:strategy:delete	Grants permission to delete policies.	write	-	-
codeartspipeline:strategy:get	Grants permission to view policies.	read	-	-
codeartspipeline:strategy:list	Grants permission to query the policy list.	list	-	-
codeartspipeline:extension:create	Grants permission to create extensions.	write	-	-
codeartspipeline:extension:update	Grants permission to update extensions.	write	-	-
codeartspipeline:extension:delete	Grants permission to delete extensions.	write	-	-
codeartspipeline:extension:get	Grants permission to view extensions.	read	-	-
codeartspipeline:extension:list	Grants permission to view the extension list.	list	-	-

Each API of CodeArts Pipeline usually supports one or more actions. **Table 5-196** lists the supported actions and dependencies.

Table 5-196 Actions and dependencies of CodeArts Pipeline APIs

API	Action	Dependency
POST /v5/{tenant_id}/api/pipeline-templates	codeartspipeline:pipelinetemplate:create	-

API	Action	Dependency
PUT /v5/{tenant_id}/api/pipeline-templates/{template_id}	codeartspipeline:pipelinetemplate:update	-
DELETE /v5/{tenant_id}/api/pipeline-templates/{template_id}	codeartspipeline:pipelinetemplate:delete	-
GET /v5/{tenant_id}/api/pipeline-templates/{template_id}	codeartspipeline:pipelinetemplate:get	-
POST /v5/{tenant_id}/api/pipeline-templates/list	codeartspipeline:pipelinetemplate:list	-
POST /v2/{domain_id}/rules/create	codeartspipeline:rule:create	-
PUT /v2/{domain_id}/rules/{rule_id}/update	codeartspipeline:rule:update	-
DELETE /v2/{domain_id}/rules/{rule_id}/delete	codeartspipeline:rule:delete	-
GET /v2/{domain_id}/rules/{rule_id}/detail	codeartspipeline:rule:get	-
GET /v2/{domain_id}/rules/query	codeartspipeline:rule:list	-
POST /v2/{domain_id}/tenant/rule-sets/create	codeartspipeline:strategy:create	-
PUT /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/update	codeartspipeline:strategy:update	-
DELETE /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/delete	codeartspipeline:strategy:delete	-

API	Action	Dependency
GET /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/detail	codeartspipeline:strategy:get	-
GET /v2/{project_id}/rule-sets/{rule_set_id}/gray/detail	codeartspipeline:strategy:get	-
GET /v2/{domain_id}/tenant/rule-sets/query	codeartspipeline:strategy:list	-
GET /v2/{project_id}/rule-sets/query	codeartspipeline:strategy:list	-
PUT /v2/{domain_id}/tenant/rule-sets/{rule_set_id}/switch	codeartspipeline:strategy:update	-
POST /v1/{domain_id}/agent-plugin/create	codeartspipeline:extension:create	-
POST /v1/{domain_id}/agent-plugin/create-draft	codeartspipeline:extension:create	-
POST /v1/{domain_id}/publisher/create	codeartspipeline:extension:create	-
POST /v1/{domain_id}/agent-plugin/edit-draft	codeartspipeline:extension:update	-
POST /v1/{domain_id}/agent-plugin/publish-draft	codeartspipeline:extension:update	-
POST /v1/{domain_id}/agent-plugin/update-info	codeartspipeline:extension:update	-
POST /v1/{domain_id}/agent-plugin/publish-plugin-bind	codeartspipeline:extension:update	-

API	Action	Dependency
POST /v1/{domain_id}/agent-plugin/publish-plugin	codeartspipeline:extension:update	-
POST /v1/{domain_id}/common/upload-plugin-icon	codeartspipeline:extension:update	-
POST /v1/{domain_id}/common/upload-publisher-icon	codeartspipeline:extension:update	-
DELETE /v1/{domain_id}/agent-plugin/delete-draft	codeartspipeline:extension:delete	-
GET /v1/{domain_id}/publisher/query-all	codeartspipeline:extension:list	-
GET /v1/{domain_id}/publisher/optional-publisher	codeartspipeline:extension:list	-
POST /v1/{domain_id}/relation/stage-plugins	codeartspipeline:extension:list	-
GET /v1/{domain_id}/relation/plugin/single	codeartspipeline:extension:list	-
POST /v1/{domain_id}/agent-plugin/query-all	codeartspipeline:extension:list	-
POST /v1/{domain_id}/agent-plugin/plugin-metrics	codeartspipeline:extension:get	-
POST /v1/{domain_id}/agent-plugin/plugin-input	codeartspipeline:extension:get	-

API	Action	Dependency
POST /v1/{domain_id}/agent-plugin/plugin-output	codeartspipeline:extension:get	-
GET /v1/{domain_id}/agent-plugin/query	codeartspipeline:extension:list	-
GET /v1/{domain_id}/agent-plugin/detail	codeartspipeline:extension:get	-
GET /v1/{domain_id}/agent-plugin/all-version	codeartspipeline:extension:list	-
DELETE /v1/{domain_id}/publisher/delete	codeartspipeline:extension:delete	-
POST /v1/{domain_id}/publisher/detail	codeartspipeline:extension:get	-
POST /v3/{domain_id}/extension/info/add	codeartspipeline:extension:create	-
POST /v3/{domain_id}/extension/info/update	codeartspipeline:extension:update	-
DELETE /v3/{domain_id}/extension/info/delete	codeartspipeline:extension:delete	-
POST /v3/{domain_id}/extension/upload	codeartspipeline:extension:update	-
GET /v3/{domain_id}/extension/detail	codeartspipeline:extension:get	-
POST /v1/{domain_id}/relation/plugins	codeartspipeline:extension:list	-

Resources

CodeArts Pipeline does not support resource-level authorization. To allow access to CodeArts Pipeline, use a wildcard (*) in the Resource element of the SCP, indicating that the SCP will be applied to all resources.

Condition

CodeArts Pipeline does not support service-specific condition keys in SCPs. It can only use global condition keys applicable to all services. For details, see Conditions Keys.

5.10.11.4 CodeArts PerfTest

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 CodeArts PerfTest, 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 CodeArts PerfTest, see **Conditions**.

The following table lists the actions that you can define in SCP statements for CodeArts PerfTest.

Table 5-197 Actions supported by CodeArts PerfTest

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codeartsperftest:privateResourceGroup:update	Grants permission to modify a private resource group.	write	privateResourceGroup	-
codeartsperftest:privateResourceGroup:list	Grants permission to view the private resource group list.	list	privateResourceGroup	-
codeartsperftest:privateResourceGroup:get	Grants permission to view a private resource group.	read	privateResourceGroup	-
codeartsperftest:privateResourceGroup:delete	Grants permission to delete a private resource group.	write	privateResourceGroup	-
codeartsperftest:privateResourceGroup:create	Grants permission to create a private resource group.	write	privateResourceGroup	-
codeartsperftest:jmeter:updateJmeterTask	Grants permission to modify a JMeter task.	write	jmeter	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codeartsperftest:jmeter:updateJmeterProject	Grants permission to modify a JMeter project.	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:listJmeterTask	Grants permission to view the JMeter task list.	list	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:listJmeterProject	Grants permission to view the JMeter project list.	list	jmeter	-
codeartsperftest:jmeter:getJmeterTask	Grants permission to view a JMeter task.	read	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:getJmeterProject	Grants permission to view a JMeter project.	get	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:executeJmeterTask	Grants permission to execute or stop a JMeter task.	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:deleteJmeterTask	Grants permission to delete a JMeter task.	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:deleteJmeterProject	Grants permission to delete a JMeter project.	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:createJmeterTask	Grants permission to create a JMeter task.	write	jmeter	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codeartsperftest:jmeter:createJmeterResource	Grants permission to create a JMeter resource, such as JMeter variable or JAR package.	write	jmeter	g:ResourceTag/<tag-key>
codeartsperftest:jmeter:createJmeterProject	Grants permission to create a JMeter project.	write	jmeter	-
codeartsperftest:cpts:updatePerfTestTask	Grants permission to modify a PerfTest task.	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:updatePerfTestProject	Grants permission to modify a PerfTest project, case, and directory.	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:listPerfTestTask	Grants permission to view the PerfTest task list.	list	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:listPerfTestProject	Grants permission to view the PerfTest project list.	list	cpts	-
codeartsperftest:cpts:getPerfTestTask	Grants permission to view a PerfTest task.	read	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:getPerfTestProject	Grants permission to view a PerfTest project.	read	cpts	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codeartsperftest:cpts:executePerfTestTask	Grants permission to execute or stop a PerfTest task.	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:deletePerfTestTask	Grants permission to delete a PerfTest task.	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:deletePerfTestProject	Grants permission to delete a PerfTest project, case, and directory.	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:createPerfTestTask	Grants permission to create a PerfTest task.	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:createPerfTestResource	Grants permissions to create a PerfTest resource, such as PerfTest case, directory, and variable.	write	cpts	g:ResourceTag/<tag-key>
codeartsperftest:cpts:createPerfTestProject	Grants permission to create a PerfTest project.	write	cpts	-
codeartsperftest::uploadFile	Grants permission to upload a file.	write	-	-
codeartsperftest::updateSlaTemplate	Grants permission to update an SLA template.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codeartsperftest::updateCronTask	Grants permission to modify a crontask.	write	-	g:ResourceTag/<tag-key>
codeartsperftest::orderPackage	Grants permission to buy a package.	write	-	-
codeartsperftest::listTag	Grants permission to view the tag list.	list	-	-
codeartsperftest::listSlaTemplate	Grants permission to view the SLA template list.	list	-	-
codeartsperftest::listPackage	Grants permission to view the purchased packages.	list	-	-
codeartsperftest::listCronTask	Grants permission to view the crontask list.	list	-	-
codeartsperftest::getTag	Grants permission to view a project's tags.	read	-	-
codeartsperftest::getSlaTemplate	Grants permission to view an SLA template.	read	-	-
codeartsperftest::getCronTask	Grants permission to view a crontask.	read	-	g:ResourceTag/<tag-key>
codeartsperftest::deleteTag	Grants permission to delete a project's tags.	tagging	-	• g:ResourceTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
codeartsperftest::deleteSlaTemplate	Grants permission to delete an SLA template.	write	-	-
codeartsperftest::deleteCronTask	Grants permission to delete a crontask.	write	-	g:ResourceTag/<tag-key>
codeartsperftest::createTag	Grants permission to create tags for a project.	tagging	-	• g:ResourceTag/<tag-key> • g:RequestTag/<tag-key> • g:TagKeys
codeartsperftest::createSlaTemplate	Grants permission to create an SLA template.	write	-	-
codeartsperftest::createCronTask	Grants permission to create a crontask.	write	-	g:ResourceTag/<tag-key>

Each API of CodeArts PerfTest usually supports one or more actions. **Table 5-198** lists the supported actions and dependencies.

Table 5-198 Actions and dependencies supported by CodeArts PerfTest APIs

API	Action	Dependencies
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/monitors	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites	codeartsperftest:jmeter:listJmeterProject	-
POST /v1/{project_id}/jmeter/test-suites	codeartsperftest:jmeter:createJmeterProject	-

API	Action	Dependencies
POST /v2/{project_id}/stress/apps	codeartsperftest:cpts:createPerfTestResource	-
POST /v1/{project_id}/periodic_package	codeartsperftest::orderPackage	-
PUT /v2/{project_id}/stress/apps/batch	codeartsperftest:cpts:updatePerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/fields	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/transactions/{transaction_id}	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/stress/agents/plugin-packages/init-multipart	codeartsperftest::uploadFile	-
GET /v1/{project_id}/all-plugin-func/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v2/{project_id}/stress/agents/batch-delete	codeartsperftest:cpts:deletePerfTestProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables	codeartsperftest:jmeter:listJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/transactions/{transaction_id}/index/{index}/css-log	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/batch-update-status	codeartsperftest:jmeter:executeJmeterTask	-
GET /v2/{project_id}/stress/apps/{id}	codeartsperftest:cpts:getPerfTestProject	-

API	Action	Dependencies
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/event	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages	codeartsperftest:jmeter:getJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}	codeartsperftest:jmeter:getJmeterProject	-
DELETE /v2/{project_id}/stress/apps/{id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/templates/file-upload/{template_id}	codeartsperftest::uploadFile	-
GET /v2/{project_id}/stress/apps	codeartsperftest:cpts:getPerfTestProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}	codeartsperftest:jmeter:deleteJmeterProject	-
GET /v1/{project_id}/all-plugin-list/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/all-plugin-req/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables/{file_variable_id}/export	codeartsperftest:jmeter:getJmeterProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages/{third_jar_id}	codeartsperftest:jmeter:deleteJmeterProject	-

API	Action	Dependencies
PUT /v1/{project_id}/monitors/{monitor_id}	codeartsperftest:cpts:updatePerfTestProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}	codeartsperftest:jmeter:deleteJmeterTask	-
GET /v1/{project_id}/order-package	codeartsperftest::orderPackage	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors/{jmeter_monitor_id}	codeartsperftest:jmeter:updateJmeterProject	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans	codeartsperftest:jmeter:createJmeterTask	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/debug	codeartsperftest:jmeter:executeJmeterTask	-
DELETE /v1/{project_id}/templates/file-delete/{template_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v2/{project_id}/stress/apps/apm/business	codeartsperftest:cpts:getPerfTestProject	-
POST /v2/{project_id}/stress/apps/batch-delete	codeartsperftest:cpts:deletePerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/thread-groups	codeartsperftest:jmeter:updateJmeterTask	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages/{third_jar_id}/export	codeartsperftest:jmeter:getJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/reports/log-outline	codeartsperftest:jmeter:getJmeterTask	-

API	Action	Dependencies
POST /v2/{project_id}/stress/apps/apm/app-info/batch-get	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/stress/agents/plugin-packages	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/plugin-json-upload/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-
GET /v1/{project_id}/test-suites/{test_suite_id}/tasks/{task_id}/link-apps	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/variable-file-download/variables/{variable_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/cce-agencies	codeartsperftest:privateResourceGroup:create	-
POST /v1/{project_id}/saveuser	codeartsperftest::listPackage	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors/{jmeter_monitor_id}	codeartsperftest:jmeter:deleteJmeterProject	-
POST /v1/{project_id}/test-suites/jmeter-upload	codeartsperftest:jmeter:createJmeterProject	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/third-jar-packages/init-multipart	codeartsperftest::uploadFile	-
POST /v1/{project_id}/cpts-agencies	codeartsperftest:privateResourceGroup:create	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables	codeartsperftest::uploadFile	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}	codeartsperftest:jmeter:updateJmeterProject	-
POST /v1/{project_id}/monitors	codeartsperftest:cpts:createPerfTestResource	-

API	Action	Dependencies
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors	codeartsperftest:jmeter:createJmeterResource	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/export	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/all-plugin-check/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks	codeartsperftest:jmeter:executeJmeterTask	-
POST /v1/{project_id}/variable-file-upload/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors	codeartsperftest:jmeter:listJmeterProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans	codeartsperftest:jmeter:listJmeterTask	-
POST /v1/{project_id}/templates/clone/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-
PUT /v2/{project_id}/stress/apps/{id}	codeartsperftest:cpts:updatePerfTestProject	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables	codeartsperftest::uploadFile	-
PUT /v1/{project_id}/variable-file-upload/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-
POST /v3/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/debug	codeartsperftest:jmeter:updateJmeterTask	-
DELETE /v2/{project_id}/stress/agents/{id}	codeartsperftest:cpts:deletePerfTestProject	-

API	Action	Dependencies
POST /v1/{project_id}/stress/agents/plugin-packages/upload	codeartsperftest::uploadFile	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/file-variables/{file_variable_id}	codeartsperftest:jmeter:deleteJmeterProject	-
POST /v1/{project_id}/stress/agents	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/stress/agents/{agent_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/csv	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/prg/{prg_id}/file/{prg_file_id}	codeartsperftest:privateResourceGroup:delete	-
GET /v1/{project_id}/search/{name}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v2/{project_id}/test-cases/{case_id}/sla/{sla_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/tasksinfos	codeartsperftest:cpts:listPerfTestTask	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/case-run-infos/{case_run_id}/detail/{detail_id}/chart	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/services/ondemand_order	codeartsperftest::listPackage	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/sla/statistic	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/{resource_type}/{resource_id}/tags	codeartsperftest::getTag	-
DELETE /v3/{project_id}/tasks/{task_id}	codeartsperftest:cpts:deletePerfTestTask	-

API	Action	Dependencies
POST /v1/{project_id}/services/ondemand_order	codeartsperftest::orderPackage	-
GET /v1/{project_id}/clusters/{cluster_id}	codeartsperftest:privateResourceGroup:get	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/case-run-infos/{case_run_id}/detail	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/templates	codeartsperftest:cpts:createPerfTestResource	-
DELETE /v1/{project_id}/tasks/{task_id}	codeartsperftest:cpts:deletePerfTestTask	-
PUT /v1/{project_id}/task-cases/{case_id}/target/{target}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/test-suites/count	codeartsperftest:cpts:listPerfTestProjectcodeartsperftest:jmeter:listJmeterProject (determine which parameter is used based on the code)	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/cases	codeartsperftest:jmeter:getJmeterTask	-
PUT /v2/{project_id}/debug/tasks/{id}/stop	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/test-suites/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/prgs/{prg_id}	codeartsperftest:privateResourceGroup:update	-
GET /v1/{project_id}/packages	codeartsperftest::listPackage	-
POST /v2/{project_id}/debug/tasks/batch-get	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/{resource_type}/tags	codeartsperftest::listTag	-

API	Action	Dependencies
DELETE /v1/{project_id}/test-suites/{test_suite_id}	codeartsperftest:cpts:deletePerfTestProject	-
PUT /v1/{project_id}/prgs/{prg_id}/ext	codeartsperftest:privateResourceGroup:update	-
POST /v1/{project_id}/{resource_type}/{resource_id}/tags/create	codeartsperftest::createTag	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/stages	codeartsperftest:cpts:getPerfTestTask	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/monitors	codeartsperftest:jmeter:listJmeterProject	-
GET /v1/{project_id}/slas	codeartsperftest::listSlaTemplate	-
GET /v1/{project_id}/test-suites/upload/processes	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/templates/{template_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/reports/details	codeartsperftest:jmeter:getJmeterTask	-
PUT /v1/{project_id}/test-suites/{test_suite_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/reports/log-outline	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/monitors-by-task/{task_id}	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/{resource_type}/{resource_id}/tags/delete	codeartsperftest::deleteTag	-

API	Action	Dependencies
POST /v1/{project_id}/domain-bindings-all/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-
GET /v1/{project_id}/cron-task/execute-time	codeartsperftest::getCronTask	-
GET /v1/{project_id}/resources/nodes/scaling/{prg_id}	codeartsperftest:privateResourceGroup:get	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/reports/details	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/monitors-by-run-id/{run_id}	codeartsperftest:cpts:getPerfTestTask	-
PUT /v1/{project_id}/sla/{sla_id}	codeartsperftest::updateSlaTemplate	-
GET /v1/{project_id}/templates/{template_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v1/{project_id}/test-suites	codeartsperftest:cpts:createPerfTestProject	-
DELETE /v1/{project_id}/task-cases/{case_id}	codeartsperftest:cpts:deletePerfTestProject	-
DELETE /v2/{project_id}/debug/tasks/{id}	codeartsperftest:cpts:deletePerfTestProject	-
GET /v2/{project_id}/test-cases/{case_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/variables/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
DELETE /v2/{project_id}/test-cases/{case_id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v2/{project_id}/test-cases/{case_id}/sla	codeartsperftest:cpts:createPerfTestResource	-
POST /v3/{project_id}/tasks	codeartsperftest:cpts:createPerfTestTask	-
PUT /v1/{project_id}/test-suites/{test_suite_id}/directory/{directory_id}	codeartsperftest:cpts:updatePerfTestProject	-
GET /v1/{project_id}/agencies/all	codeartsperftest:privateResourceGroup:get	-

API	Action	Dependencies
GET /v1/{project_id}/tasks/history-run-list/{task_id}	codeartsperftest:cpts:listPerfTestTask	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/details/export	codeartsperftest:cpts:getPerfTestTask	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/detail	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/{project_id}/templates/swagger-import/{test_suite_id}/contract-id/{contract_id}/model-id/{model_id}	codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/variables/{test_suite_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/test-suites/{test_suit_id}/tasks/batch-update-task-status	codeartsperftest:cpts:executePerfTestTask	-
GET /v1/{project_id}/variables/{variable_type}/test-suites/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/cron-task	codeartsperftest::listCronTask	-
POST /v1/{project_id}/tasks	codeartsperftest:cpts:createPerfTestTask	-
GET /v1/{project_id}/test-suites	codeartsperftest:cpts:listPerfTestProject	-
POST /v1/{project_id}/prg/{prg_id}/upload	codeartsperftest::uploadFile	-
POST /v1/{project_id}/{resource_type}/resource-instances/count	codeartsperftest::listTag	-
POST /v1/{project_id}/test-suites/download	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/all-tasks/{test_suite_id}	codeartsperftest:cpts:listPerfTestTask	-
GET /v1/{project_id}/tasks/{task_id}	codeartsperftest:cpts:getPerfTestTask	-

API	Action	Dependencies
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/multi-third-jar-packages/{third_jar_id}	codeartsperftest::uploadFile	-
GET /v1/{project_id}/cron-task/{cron_task_id}	codeartsperftest::getCronTask	-
POST /v1/{project_id}/prgs	codeartsperftest:privateResourceGroup:create	-
GET /v2/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/details/export	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/monitor-list/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/invite-features	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/prgs/{prg_id}	codeartsperftest:privateResourceGroup:get	-
POST /v1/{project_id}/packages	codeartsperftest::orderPackage	-
DELETE /v1/{project_id}/prgs/{prg_id}/ext/{ext_id}	codeartsperftest:privateResourceGroup:delete	-
GET /v1/{project_id}/tasks/history-run-info/{run_id}	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/cron-task/{cron_task_id}	codeartsperftest::deleteCronTask	-
GET /v1/{project_id}/test-suites/{test_suite_id}/directory	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/event/sla	codeartsperftest:cpts:getPerfTestTask	-
POST /v2/{project_id}/test-cases/batch-delete	codeartsperftest:cpts:deletePerfTestProject	-
PUT /v1/{project_id}/monitors-by-task/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-

API	Action	Dependencies
GET /v1/{project_id}/pods-info/{exec_info_id}	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/clusters	codeartsperftest:privateResourceGroup:list	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/reports	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/index/{index}/debug-result	codeartsperftest:cpts:getPerfTestTask	-
PUT /v3/{project_id}/tasks/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-
DELETE /v2/{project_id}/test-cases/{case_id}/sla/{sla_id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/templates/swagger-insert/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-
DELETE /v1/{project_id}/prgs/{prg_id}/delete_forced	codeartsperftest:privateResourceGroup:delete	-
GET /v2/{project_id}/test-cases/{case_id}/slas	codeartsperftest:cpts:getPerfTestProject	-
PUT /v1/{project_id}/test-suites/{test_suite_id}/domain-binding/{domain_binding_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/test-suites/{test_suite_id}/tasks/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/index/{index}/css-log	codeartsperftest:cpts:getPerfTestTask	-

API	Action	Dependencies
POST /v2/{project_id}/test-suites/{test_suite_id}/cases/{case_id}/debug	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/cron-task	codeartsperftest::createCronTask	-
POST /v1/{project_id}/templates/upload/{template_id}	codeartsperftest:cpts:createPerfTestResource	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/icon-metrics	codeartsperftest:cpts:getPerfTestTask	-
GET /v2/{project_id}/debug/tasks	codeartsperftest:cpts:getPerfTestProject	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/cases	codeartsperftest:cpts:getPerfTestTask	-
GET /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/event	codeartsperftest:cpts:getPerfTestTask	-
PUT /v1/{project_id}/cron-task/{cron_task_id}	codeartsperftest::updateCronTask	-
GET /v2/{project_id}/monitor-list/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/test-suites/{test_suit_id}/tasks/{task_id}/test-cases	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/test-suites/{test_suite_id}/directory/{directory_id}	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/prgs/{prg_id}/ext	codeartsperftest:privateResourceGroup:create	-
GET /v2/{project_id}/tasks/{task_id}	codeartsperftest:cpts:getPerfTestTask	-
PUT /v1/{project_id}/domain-bindings-all/{test_suite_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/sla	codeartsperftest::createSlaTemplate	-

API	Action	Dependencies
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/variables	codeartsperftest:jmeter:getJmeterTask	-
POST /v1/{project_id}/{resource_type}/resource-instances/filter	codeartsperftest::listTag	-
POST /v1/{project_id}/test-suites/{test_suite_id}/directory	codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/cron-task/{cron_task_id}/status	codeartsperftest::updateCronTask	-
GET /v1/{project_id}/prgs	codeartsperftest:privateResourceGroup:list	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/reports/log-outline	codeartsperftest:cpts:getPerfTestTask	-
DELETE /v1/{project_id}/sla/{sla_id}	codeartsperftest::deleteSlaTemplate	-
PUT /v1/{project_id}/tasks/{task_id}	codeartsperftest:cpts:updatePerfTestTask	-
GET /v1/{project_id}/sla/{sla_id}	codeartsperftest::getSlaTemplate	-
DELETE /v1/{project_id}/prgs/{prg_id}	codeartsperftest:privateResourceGroup:delete	-
GET /v1/{project_id}/domain-bindings-all/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
POST /v3/{project_id}/test-suites/{test_suite_id}/cases/{case_id}/debug	codeartsperftest:cpts:updatePerfTestProject	-
POST /v1/{project_id}/variable-file-upload/init-multipart	codeartsperftest::uploadFile	-
POST /v1/{project_id}/templates/swagger-upload/{test_suite_id}	codeartsperftest:cpts:createPerfTestResource	-
GET /v2/{project_id}/test-cases/{case_id}/rel-temp-tasks	codeartsperftest:cpts:getPerfTestTask	-

API	Action	Dependencies
POST /v2/{project_id}/test-cases	codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/stages	codeartsperftest:cpts:updatePerfTestTask	-
PUT /v2/{project_id}/test-cases/{case_id}	codeartsperftest:cpts:updatePerfTestProject	-
POST /v2/{project_id}/test-cases/batch-run	codeartsperftest:cpts:executePerfTestTask	-
POST /v1/{project_id}/task-cases	codeartsperftest:cpts:createPerfTestResource	-
GET /v1/{project_id}/prg/{prg_id}/files	codeartsperftest:privateResourceGroup:get	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/history-tasks	codeartsperftest:jmeter:getJmeterTask	-
GET /v1/{project_id}/all-templates/{test_suite_id}	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/prg/regions	codeartsperftest:privateResourceGroup:get	-
GET /v2/{project_id}/task-run-infos/{task_run_id}/case-run-infos/{case_run_id}/detail/{detail_id}/chart	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/{project_id}/test-suites/{test_suite_id}/tasks/{task_id}/cases/{case_id}/debug	codeartsperftest:cpts:updatePerfTestProject	-
DELETE /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/multi-third-jar-packages	codeartsperftest::uploadFile	-
POST /v1/{project_id}/domain-binding/{domain_binding_id}	codeartsperftest:cpts:deletePerfTestProject	-

API	Action	Dependencies
DELETE /v1/{project_id}/test-suites/upload	codeartsperftest:cpts:createPerfTestProject&&codeartsperftest:cpts:createPerfTestResource	-
PUT /v1/{project_id}/monitors/{monitor_id}	codeartsperftest:cpts:deletePerfTestProject	-
DELETE /v1/{project_id}/prgs/{prg_id}/ratio	codeartsperftest:privateResourceGroup:update	-
DELETE /v1/{project_id}/templates/{template_id}	codeartsperftest:cpts:deletePerfTestProject	-
GET /v1/{project_id}/variables	codeartsperftest:cpts:deletePerfTestProject	-
POST /v1/{project_id}/prg/upload/{upload_id}/processes	codeartsperftest:privateResourceGroup:get	-
GET /v1/{project_id}/variables/{test_suite_id}	codeartsperftest:cpts:createPerfTestProject	-
POST /v1/{project_id}/test-suites/{test_suit_id}/tasks/{task_id}/cron-tasks	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/{project_id}/column/check-name	codeartsperftest:cpts:getPerfTestProject	-
GET /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/cron-tasks	codeartsperftest:jmeter:getJmeterTask	-
PUT /v1/{project_id}/jmeter/test-suites/{jmeter_project_id}/test-plans/{test_plan_id}/tasks/{task_run_info_id}/update-report-name	codeartsperftest:jmeter:getJmeterTask	-
PUT /v1/{project_id}/task-run-infos/{task_run_id}/update-report-name	codeartsperftest:cpts:getPerfTestTask	-
POST /v1/test-suites/upload-java/json-file	codeartsperftest:cpts:createPerfTestProject codeartsperftest:cpts:createPerfTestResource	-
POST /v1/test-suites/upload-java/init-multipart	codeartsperftest::uploadFile	-

API	Action	Dependencies
POST /v1/test-suites/upload-java/test-suites/{test_suite_id}	codeartsperftest::uploadFile	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-199**, 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 CodeArts PerfTest.

Table 5-199 Resource types supported by CodeArts PerfTest

Resource Type	URN
cpts	codeartsperftest:<region>:<account-id>:cpts:<test-suite-name>
jmeter	codeartsperftest:<region>:<account-id>:jmeter:<test-suite-name>
privateResourceGroup	codeartsperftest:<region>:<account-id>:privateResourceGroup:<resource-group-name>

Conditions

CodeArts PerfTest 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.

5.10.12 Business Applications

5.10.12.1 Domain Name Service (DNS)

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 topic 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 (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 SCP 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 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 DNS, 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 DNS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for DNS.

Table 5-200 Actions supported by DNS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dns:zone:list	Grants permission to list the zones.	list	zone *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dns:zone:create	Grants permission to create a zone.	write	zone *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dns:zone:createBatchPublicZonesByName	Grants permission to create zones in batches.	write	zone *	-
			-	g:EnterpriseProjectId
dns:zone:get	Grants permission to query a zone.	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:update	Grants permission to update a zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:delete	Grants permission to delete a zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:associaterouter	Grants permission to associate VPCs with a private zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:disassociaterouter	Grants permission to disassociate VPCs from a private zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dns:zone:setProxyPattern	Grants permission to set the recursive resolution proxy for a private zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:transfer	Grants permission to transfer a public zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:list	Grants permission to list the record sets.	list	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:create	Grants permission to create a record set.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:recordset:get	Grants permission to query a record set.	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:update	Grants permission to update a record set.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:recordset:delete	Grants permission to delete a record set.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:zone:setStatus	Grants permission to set the zone status.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:setStatus	Grants permission to set the status of a record set.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• dns:RecordSetNames • dns:RecordSetTypes
dns:ptr:list	Grants permission to list the PTR records.	list	ptr *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dns:ptr:get	Grants permission to query a PTR record.	read	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:ptr:create	Grants permission to create a PTR record.	write	ptr *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
dns:ptr:update	Grants permission to update a PTR record.	write	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dns:ptr:delete	Grants permission to delete a PTR record.	write	ptr *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:tag:get	Grants permission to query tags of a zone.	read	zone	-
dns:tag:get	Grants permission to query tags of a zone.	read	ptr	-
dns:tag:set	Grants permission to add a tag to a zone.	tagging	zone	g:ResourceTag/<tag-key>
dns:tag:set	Grants permission to add a tag to a zone.	tagging	ptr	g:ResourceTag/<tag-key>
dns:zone:createRetrieval	Grants permission to retrieve a domain name.	write	-	-
dns:zone:getRetrieval	Grants permission to query the domain name 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 name servers.	list	-	-
dns:nameserver:getZoneNameServer	Grants permission to query DNS servers for public zones.	read	-	-
dns:quota:list	Grants permission to list quotas.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dns:recordset:getPrivateRecordSetImport	Grants permission to query private zone record set import.	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:getPrivateRecordSetImportTemplate	Grants permission to download the template for importing private zone record sets.	read	-	-
dns:recordset:createPrivateRecordSetImport	Grants permission to create a private zone record set import task.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:deletePrivateRecordSetImportTask	Grants permission to delete a private zone record set import task.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:createPublicRecordSetImport	Grants permission to create a public zone record set import task.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:getPublicRecordSetImport	Grants permission to query public zone record set import.	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:recordset:getPublicRecordSetImportTemplate	Grants permission to download the template for importing public zone record sets.	read	-	-
dns:recordset:deletePublicRecordSetImportTask	Grants permission to delete a public zone record set import task.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:getExport	Grants permission to export zones.	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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 *	-
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 an endpoint.	write	endpoint *	-
dns:endpoint:list	Grants permission to list the endpoints.	list	endpoint *	-
dns:endpoint:get	Grants permission to query an endpoint.	read	endpoint *	-
dns:endpoint:update	Grants permission to update an endpoint.	write	endpoint *	-
dns:endpoint:delete	Grants permission to delete an endpoint.	write	endpoint *	-
dns:endpoint:createIpaddress	Grants permission to bind an IP address to an endpoint.	write	endpoint *	-
dns:endpoint:deleteIpaddress	Grants permission to unbind an IP address from an endpoint.	write	endpoint *	-
dns:endpoint:listIpaddresses	Grants permission to list IP addresses bound to an endpoint.	list	endpoint *	-
dns:endpoint:listVpcs	Grants permission to list the VPCs associated with an endpoint.	list	endpoint *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dns:resolverRule:create	Grants permission to create an endpoint rule to route queries originating from your VPC out of the VPC.	write	resolverRule *	-
dns:resolverRule:list	Grants permissions to list endpoint rules.	list	resolverRule *	-
dns:resolverRule:get	Grants permission to query an endpoint rule.	read	resolverRule *	-
dns:resolverRule:update	Grants permissions to update an endpoint rule.	write	resolverRule *	-
dns:resolverRule:delete	Grants permissions to delete an endpoint rule.	write	resolverRule *	-
dns:resolverRule:associaterouter	Grants permission to associate a VPC with an endpoint rule.	write	resolverRule *	-
dns:resolverRule:disassociaterouter	Grants permission to disassociate a VPC from an endpoint rule.	write	resolverRule *	-
dns:zone:enableDnssecConfig	Grants permission to enable DNSSEC for a zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:disableDnssecConfig	Grants permission to disable DNSSEC for a zone.	write	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:getDnssecConfig	Grants permission to query DNSSEC for a zone.	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
dns:zone:listPublicZoneBatchOperationRecords	Grants permission to list batch operation records of public zones.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
dns:zone:getPublicZoneBatchOperationResult	Grants permission to download failed batch operations on public zones.	read	-	-
dns:recordset:batchImportPublicRecordSet	Grants permission to import public zone record sets in batches.	write	-	-
dns:zone:createAuthorizeTxtRecord	Grant permissions to authorize a domain name.	write	-	-
dns:zone:getAuthorizeTxtRecord	Grants permission to query the authorization status of a domain name.	read	-	-
dns:zone:getDomainDetection	Grants permission to query public domain name resolution diagnosis results.	read	zone *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Each API of DNS usually supports one or more actions. **Table 5-201** lists the supported actions and dependencies.

Table 5-201 Actions and dependencies supported by DNS APIs

API	Action	Dependencies
GET /v2/zones	dns:zone:list	-
POST /v2/zones	dns:zone:create	• dns:tag:set • dns:quota:list
GET /v2/zones/{zone_id}	dns:zone:get	-
PATCH /v2/zones/{zone_id}	dns:zone:update	-
DELETE /v2/zones/{zone_id}	dns:zone:delete	-

API	Action	Dependencies
GET /v2/zones/{zone_id}/nameservers	dns:zone:get	-
GET /v2/zones	dns:zone:list	-
POST /v2/zones	dns:zone:create	• vpc:vpcs:get • dns:tag:set • dns:quota:list
GET /v2/zones/{zone_id}	dns:zone:get	-
PATCH /v2/zones/{zone_id}	dns:zone:update	-
DELETE /v2/zones/{zone_id}	dns:zone:delete	-
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
GET /v2/zones/{zone_id}/recordsets	dns:recordset:list	-
POST /v2/zones/{zone_id}/recordsets	dns:recordset:create	dns:quota:list
GET /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:get	-
PUT /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:update	-
DELETE /v2/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:delete	-
GET /v2/recordsets	dns:recordset:list	-

API	Action	Dependencies
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	dns:quota:list
GET /v2.1/zones/{zone_id}/recordsets	dns:recordset:list	-
GET /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:get	-
PUT /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:update	-
DELETE /v2.1/zones/{zone_id}/recordsets/{recordset_id}	dns:recordset:delete	-
PUT /v2.1/recordsets/{recordset_id}/statuses/set	dns:recordset:setStatus	-
POST /v2.1/zones/{zone_id}/recordsets/batch/lines	dns:recordset:create	dns:quota:list
PUT /v2.1/zones/{zone_id}/recordsets	dns:recordset:update	-
DELETE /v2.1/zones/{zone_id}/recordsets	dns:recordset:delete	-
GET /v2/reverse/floatingips	dns:ptr:list	-
GET /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:get	-
PATCH /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:create	• eip:publicIps:get • dns:tag:set • dns:quota:list

API	Action	Dependencies
PATCH /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:update	-
PATCH /v2/reverse/floatingips/{region}:{floatingip_id}	dns:ptr:delete	-
GET /v2/{project_id}/{resource_type}/tags	dns:tag:get	-
GET /v2/{project_id}/{resource_type}/{resource_id}/tags	dns:tag:get	-
POST /v2/{project_id}/{resource_type}/{resource_id}/tags	dns:tag:set	-
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	-

API	Action	Dependencies
GET /v2/nameservers	dns:nameserver:list	-
GET /v2/quotamg/dns/quotas	dns:quota:list	-
POST /v2.1/linegroups	dns:lineGroup:create	dns:quota:list
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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-202**, 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 DNS.

Table 5-202 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>

Resource Type	URN
ptr	dns:<region>:<account-id>:ptr:<ptr-id>

Conditions

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

- A key in the Condition element of a 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, dns:) only apply to operations of the DNS service. For details, see **Table 5-203**.
  - 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.

The following table lists the condition keys that you can define in SCPs for DNS. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-203 Service-specific condition keys supported by DNS

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
dns:RecordSetNames	string	Multivalued	Filters access by record set name. All letters in the record set name must be lowercase and cannot contain a period at the end.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
dns:RecordSetTypes	string	Multivalued	Filters access by record set type. The value can be **A**, **AAAA**, **MX**, **CNAME**, **TXT**, **NS**, **CAA**, or **SRV**.

5.10.12.2 Workspace

The Organizations service 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.

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 edit a custom SCP policy, see Creating an SCP.

Actions

Actions are specific operations that are allowed or denied in an identity policy 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 Workspace, 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 condition keys defined by Workspace, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Workspace.

Table 5-204 Actions supported by Workspace

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:authConfigs:get	Grants permission to query the configuration of the authentication login mode.	read	-	-
workspace:authConfigs:update	Grants permission to update authentication policy configurations.	write	-	-
workspace:assistAuthConfigs:get	Grants permission to query auxiliary authentication configurations.	read	-	-
workspace:assistAuthConfigs:update	Grants permission to update auxiliary authentication configurations.	write	-	-
workspace:jobs:retry	Grants permission to retry a task.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:quotas:get	Grants permission to query tenant quotas.	read	-	-
workspace:tenants:getRoles	Grants permission to query tenant roles.	read	-	-
workspace:tenants:ListConfig	Grants permission to query customized tenant configurations.	list	-	-
workspace:tenants:updateConfig	Grants permission to modify customized tenant configurations.	write	-	-
workspace:natMappings:getConfig	Grants permission to query NAT mapping configuration items of a tenant.	read	-	-
workspace:natMappings:updateConfig	Grants permission to modify NAT mapping configuration items of a tenant.	write	-	-
workspace:tenants:get	Grants permission to query Huawei Cloud Workspace details.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:tenants:open	Grants permission to subscribe to Huawei Cloud Workspace.	write	-	workspace:AccessMode
workspace:tenants:delete	Grants permission to unsubscribe from Huawei Cloud Workspace.	write	-	-
workspace:tenants:update	Grants permission to modify attributes of Huawei Cloud Workspace.	write	-	workspace:AccessMode
workspace:tenants:getLockStatus	Grants permission to query whether Huawei Cloud Workspace is locked.	read	-	-
workspace:tenants:unlock	Grants permission to unlock Huawei Cloud Workspace.	write	-	-
workspace:agencies:create	Grants permission to create an agency.	write	-	-
workspace:agencies:get	Grants permission to query agencies.	read	-	-
workspace:desktops:createAiAccelerateJob	Grants permission to create a rendering acceleration task.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:getAiAccelerateJob	Grants permission to query rendering acceleration tasks.	read	-	-
workspace:desktops:getSysPrepInfo	Grants permission to query Sysprep details.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:checkBatchChangeImage	Grants permission to verify batch image switchover.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:listDesktopNamePolicies	Grants permission to query desktop naming policies.	list	-	-
workspace:tenants:createDesktopNamePolicy	Grants permission to create a desktop naming policy.	write	-	-
workspace:tenants:updateDesktopNamePolicy	Grants permission to update a desktop naming policy.	write	-	-
workspace:tenants:batchDeleteDesktopNamePolicies	Grants permission to delete desktop naming policies in batches.	write	-	-
workspace:desktopPools:create	Grants permission to create a desktop pool.	write	desktopPool *	-
			user	-
			userGroup	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktopPools:list	Grants permission to query desktop pools.	list	desktopPool *	-
workspace:desktopPools:update	Grants permission to modify desktop pool attributes.	write	desktopPool *	-
workspace:desktopPools:delete	Grants permission to delete a desktop pool.	write	desktopPool *	-
workspace:desktopPools:get	Grants permission to query desktop pool details.	read	desktopPool *	-
workspace:desktopPools:expand	Grants permission to expand the desktop pool capacity.	write	desktopPool *	-
workspace:desktopPools:resize	Grants permission to change desktop pool specifications.	write	desktopPool *	-
workspace:desktopPools:rebuild	Grants permission to recompose the system disk of a desktop pool.	write	desktopPool *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktopPools:batchAddVolumes	Grants permission to add disks to desktop pools in batches.	write	desktopPool *	-
workspace:desktopPools:batchDeleteVolumes	Grants permission to delete disks from desktop pools in batches.	write	desktopPool *	-
workspace:desktopPools:batchExpandVolumes	Grants permission to expand the capacity of disks in batches in a desktop pool.	write	desktopPool *	-
workspace:desktopPools:operate	Grants permission to perform operations on a desktop pool.	write	desktopPool *	-
workspace:desktopPools:listUsers	Grants permission to query users and user groups authorized by the desktop pool.	list	desktopPool *	-
workspace:desktopPools:authorizeUsers	Grants permission to authorize users and user groups to access a desktop pool.	write	desktopPool *	-
			user	-
			userGroup	-
workspace:desktopPools:listDesktops	Grants permission to query desktop information in desktop pools.	list	desktopPool *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktopPools:listScriptTasks	Grants permission to query the script execution task list of a desktop pool.	list	desktopPool *	-
workspace:desktopPools:executeScripts	Grants permission to execute desktop pool scripts in batches.	write	desktopPool *	-
			script	-
workspace:desktopPools:sendNotifications	Grants permission to send notifications.	write	desktopPool *	-
workspace:desktops:export	Grants permission to export a desktop list.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:create	Grants permission to create a desktop.	write	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • workspace:AssociatePublicIp • workspace:AccessMode
workspace:desktops:list	Grants permission to query desktops.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:update	Grants permission to update desktop information.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:delete	Grants permission to delete a desktop.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:get	Grants permission to query desktop details.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDelete	Grants permission to delete desktops in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:logoff	Grants permission to log out of desktops in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetail	Grants permission to query desktop details.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:operate	Grants permission to perform operations on a desktop.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:resize	Grants permission to change specifications.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:getConnectStatus	Grants permission to query desktop login status statistics.	read	-	-
workspace:desktops:ListStatus	Grants permission to query desktop login statuses.	list	-	-
workspace:desktops:rebuild	Grants permission to recompose desktops.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getActions	Grants permission to query desktop power-on/off information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createConsole	Grants permission to obtain the URL for remote login to the console.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:updateSids	Grants permission to update a desktop SID.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:rejoinDomain	Grants permission to rejoin the AD domain.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createImage	Grants permission to convert a desktop to an image.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDetach	Grants permission to unbind users in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:detach	Grants permission to unbind a user.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:attach	Grants permission to assign a desktop to a user.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getNetwork	Grants permission to query desktop network information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeNetwork	Grants permission to switch the desktop network.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:exclusiveHosts:listDesktops	Grants permission to query exclusive desktop details.	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:desktops:listAll	Grants permission to query general-purpose desktops and rendering desktops.	list	desktop *	-
workspace:desktopAssociate:listDiscoverVmInfo	Grants permission to query the list of VMs that can be managed.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktopAssociate:startTask	Grants permission to start a VM management task.	write	-	-
workspace:desktopAssociate:switchScanTask	Grants permission to enable a management scanning task.	write	-	-
workspace:desktopAssociate:getScanTaskSwitch	Grants permission to query management scanning tasks.	read	-	-
workspace:desktops:setMaintenanceMode	Grants permission to set the desktop administrator maintenance mode in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:prepAttachUsers	Grants permission to pre-assign desktops to users in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchAttachUsers	Grants permission to assign desktops to users in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeUsername	Grants permission to change usernames associated with desktops in Windows AD.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:sendNotifications	Grants permission to send notifications.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:migrate	Grants permission to migrate desktops.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listAgents	Grants permission to query the list of desktops with installed agents.	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchInstallAgents	Grants permission to install agents for desktops in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listTags	Grants permission to query desktop tags.	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:tag	Grants permission to create a desktop tag.	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:untag	Grants permission to delete a desktop tag.	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:listProjectTags	Grants permission to query project tags.	list	-	-
workspace:desktops:operateTags	Grants permission to add or delete tags in batches.	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listByTags	Grants permission to filter desktops by tag.	list	-	-
workspace:exclusiveHosts:create	Grants permission to create an exclusive host.	write	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:list	Grants permission to query exclusive hosts.	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:check	Grants permission to check whether exclusive hosts can be created.	write	-	-
workspace:exclusiveHosts:get	Grants permission to query exclusive host details.	read	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:update	Grants permission to update exclusive host information.	write	exclusiveHost *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:exclusiveHosts:delete	Grants permission to delete an exclusive host.	write	exclusiveHost *	g:EnterpriseProjectId
workspace:mkp:listImages	Grants permission to query images in KooGallery.	list	-	-
workspace:mkp:listCommodityInfos	Grants permission to query product information in KooGallery.	list	-	-
workspace:mkp:createOrder	Grants permission to create a product order in KooGallery.	write	-	-
workspace:mkp:listListProductReserve	Grants permission to query the KooGallery inventory.	list	-	-
workspace:mkp:listCommodityDetails	Grants permission to query product details in KooGallery.	list	-	-
workspace:mkp:listRelationCommodityDetails	Grants permission to query associated products.	list	-	-
workspace:mkp:listCommodityAgreements	Grants permission to query product agreements in KooGallery.	list	-	-
workspace:networks:listEips	Grants permission to query EIPs.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:networks:createEips	Grants permission to create an EIP.	write	-	-
workspace:networks:bindEips	Grants permission to bind an EIP.	write	-	-
workspace:networks:unbindEips	Grants permission to unbind an EIP.	write	-	-
workspace:networks:getEipQuota	Grants permission to query EIP quotas.	read	-	-
workspace:networks:ListNatGateways	Grants permission to query NAT gateways.	list	-	-
workspace:orders:create	Grants permission to place a yearly/monthly order.	write	-	• workspace:CreateOrderType • workspace:AssociatePublicIp • workspace:AccessMode
workspace:orders:change	Grants permission to create a change order.	write	-	workspace:ChangeOrderType
workspace:orders:batchInquiry	Grants permission to inquire prices in batches.	write	-	-
workspace:quotas:check	Grants permission to verify quotas.	write	-	-
workspace:renderDesktops:create	Grants permission to create a rendering desktop.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:renderDesktops:delete	Grants permission to delete a rendering desktop.	write	-	-
workspace:renderDesktops:list	Grants permission to query rendering desktops.	list	-	-
workspace:renderDesktops:action	Grants permission to perform operations on a rendering desktop.	write	-	-
workspace:scheduledTasks:list	Grants permission to query scheduled tasks.	list	scheduledTask *	-
workspace:scheduledTasks:create	Grants permission to create a scheduled task.	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:get	Grants permission to query scheduled task details.	read	scheduledTask *	-
workspace:scheduledTasks:update	Grants permission to update a scheduled task.	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:scheduledTasks:delete	Grants permission to delete a scheduled task.	write	scheduledTask *	-
workspace:scheduledTasks:getFuture	Grants permission to query the future execution time of a scheduled task.	read	-	-
workspace:scheduledTasks:batchDelete	Grants permission to delete scheduled tasks in batches.	write	scheduledTask *	-
workspace:scheduledTasks:listRecords	Grants permission to query the execution records of a scheduled task.	list	scheduledTask *	-
workspace:scheduledTasks:getRecord	Grants permission to query details about scheduled task execution records.	read	scheduledTask *	-
workspace:scheduledTasks:exportRecords	Grants permission to export details about scheduled task execution records.	list	scheduledTask *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:subscribeSharer	Grants permission to subscribe to collaborative resources.	write	user *	-
workspace:desktops:addSubResources	Grants permission to purchase depended desktop resources.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSubResources	Grants permission to delete depended desktop resources.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createSnapshots	Grants permission to create a desktop snapshot.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getSnapshots	Grants permission to query desktop snapshots.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSnapshots	Grants permission to delete a desktop snapshot.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:restoreBySnapshot	Grants permission to restore desktops using desktop snapshots.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:statistics:listDesktopStatus	Grants permission to collect statistics on desktop statuses.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:statistics:getUnused	Grants permission to query desktops that are not in use in a specified period.	read	-	-
workspace:statistics:getUsed	Grants permission to query the desktop usage duration.	read	-	-
workspace:bindingPolicies:export	Grants permission to export information about terminal-desktop binding to an Excel file.	list	-	-
workspace:bindingPolicies:getConfig	Grants permission to query a terminal-desktop binding configuration.	read	-	-
workspace:bindingPolicies:createConfig	Grants permission to configure terminal-desktop binding.	write	-	-
workspace:bindingPolicies:get	Grants permission to query terminal-desktop binding configurations.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:bindingPolicies:add	Grants permission to add a terminal-desktop binding configuration.	write	-	-
workspace:bindingPolicies:update	Grants permission to modify a terminal-desktop binding configuration.	write	-	-
workspace:bindingPolicies:delete	Grants permission to delete a terminal-desktop binding configuration.	write	-	-
workspace:volumes:delete	Grants permission to delete a desktop data disk.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchAdd	Grants permission to add a desktop disk.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchExpand	Grants permission to expand a desktop disk.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:wdh:getType	Grants permission to query Workspace host types.	read	wdh *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:wdh:get	Grants permission to query Workspace hosts.	read	wdh *	g:EnterpriseProjectId
workspace:desktops:getRemoteAssistance	Grants permission to query remote assistance information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createRemoteAssistance	Grants permission to create remote assistance.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:cancelRemoteAssistance	Grants permission to cancel remote assistance.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:add	Grants permission to add disks to a single desktop.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:expand	Grants permission to expand disk capacity.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:listDssPoolsDetail	Grants permission to obtain the dedicated distributed storage pool list.	list	-	-
workspace:common:listTimezones	Grants permission to query the time zone configuration.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:connections:securityExport	Grants permission to export connection records.	list	-	-
workspace:images:list	Grants permission to query supported images.	list	-	-
workspace:policyGroups:import	Grants permission to import a policy group.	write	-	-
workspace:accessPolicies:create	Grants permission to create an access policy.	write	-	-
workspace:accessPolicies:get	Grants permission to query access policies.	read	-	-
workspace:accessPolicies:delete	Grants permission to delete a specified access policy.	write	-	-
workspace:accessPolicies:getTarget	Grants permission to query objects to which a specified access policy is applied.	read	-	-
workspace:accessPolicies:updateTarget	Grants permission to update objects to which a specified access policy is applied.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:products:listDesktopProducts	Grants permission to query the list of available product packages.	list	-	-
workspace:products:listSharerProducts	Grants permission to query the list of collaboration packages.	list	-	-
workspace:products:listInternetProducts	Grants permission to query the list of Internet access packages.	list	-	-
workspace:availabilityZones:list	Grants permission to query AZs where Workspace is available.	list	-	-
workspace:userGroups:export	Grants permission to export a user group.	list	userGroup *	-
workspace:users:export	Grants permission to export a user.	list	user *	-
workspace:users:import	Grants permission to import a user.	write	user *	-
workspace:userGroups:exportUsers	Grants permission to export users in a user group.	list	userGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:operate	Grants permission to operators (locking, unlocking, and resetting passwords).	write	user *	-
workspace:users:randomPassword	Grants permission to reset a random password for a user.	write	user *	-
workspace:users:deleteOtps	Grants permission to unbind an OTP device.	write	user *	-
workspace:users:resendEmail	Grants permission to resend an email.	write	user *	-
workspace:connections:securityList	Grants permission to query connection information.	list	-	-
workspace:connections:listOnlineUsers	Grants permission to query the number of login users.	list	-	-
workspace:userGroups:list	Grants permission to query user groups.	list	userGroup *	-
workspace:userGroups:create	Grants permission to create a user group.	write	userGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:userGroups:batchDelete	Grants permission to delete user groups in batches.	write	userGroup *	-
workspace:userGroups:delete	Grants permission to delete a desktop user group.	write	userGroup *	-
workspace:userGroups:update	Grants permission to modify user group information.	write	userGroup *	-
workspace:userGroups:operate	Grants permission to perform operations on a user group.	write	userGroup *	-
			user *	-
workspace:userGroups:getUsers	Grants permission to query users in a user group.	list	userGroup *	-
workspace:jobs:listSubJobs	Grants permission to query subtasks.	list	-	-
workspace:jobs:deleteSubJobRecords	Grants permission to delete a subtask record.	write	-	-
workspace:ou:get	Grants permission to query OU information.	list	-	-
workspace:ou:create	Grants permission to add OU information.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:ou:delete	Grants permission to delete OU information.	write	-	-
workspace:ou:update	Grants permission to update OU information.	write	-	-
workspace:policyGroups:list	Grants permission to query policy groups.	list	policyGroup *	-
workspace:policyGroups:create	Grants permission to add a policy group.	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:delete	Grants permission to delete a policy group.	write	policyGroup *	-
workspace:policyGroups:get	Grants permission to query policy groups.	read	policyGroup *	-
workspace:policyGroups:update	Grants permission to modify a policy group.	write	policyGroup *	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:export	Grants permission to export a policy group.	list	policyGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:policyGroups:listPolicies	Grants permission to query policy items of a policy group.	list	policyGroup *	-
workspace:policyGroups:updatePolicies	Grants permission to modify policy items of a policy group.	write	policyGroup *	-
workspace:policyGroups:listTargets	Grants permission to query objects to which the policy group is applied.	list	policyGroup *	-
workspace:policyGroups:updateTargets	Grants permission to modify objects to which the policy group is applied.	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:listDetail	Grants permission to query details about policy groups.	list	policyGroup *	-
workspace:policyGroups:getOriginalPolicies	Grants permission to query initial policy items.	read	policyGroup *	-
workspace:users:list	Grants permission to query users.	list	user *	-
workspace:users:create	Grants permission to create a user.	write	user *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:delete	Grants permission to delete a specified user.	write	user *	-
workspace:users:get	Grants permission to query user details.	read	user *	-
workspace:users:update	Grants permission to modify user information.	write	user *	-
workspace:users:batchDelete	Grants permission to delete users in batches.	write	user *	-
workspace:users:resetPassword	Grants permission to reset a user password.	write	user *	-
workspace:users:checkResetPasswordToken	Grants permission to verify tokens for resetting passwords of domain users.	write	user *	-
workspace:users:getTemplate	Grants permission to download a user template.	read	-	-
workspace:users:checkExist	Grants permission to check whether the user exists.	write	user *	-
workspace:users:listOtps	Grants permission to query OTP devices.	list	user *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:getImportTemplate	Grants permission to download a created user template.	read	-	-
workspace:users:batchCreate	Grants permission to create users in batches.	write	user *	-
workspace:products:listVolumeProducts	Grants permission to query disk products.	list	-	-
workspace:tenants:listExportTasks	Grants permission to query export tasks.	list	-	-
workspace:tenants:deleteExportTasks	Grants permission to delete export task records in batches.	write	-	-
workspace:tenants:exportData	Grants permission to download an exported file.	read	-	-
workspace:statistics:listAlarm	Grants permission to query alarms.	list	-	-
workspace:statistics:getAlarm	Grants permission to query the number of alarms.	read	-	-
workspace:statistics:getGrowthRate	Grants permission to query the chain value of a metric.	read	-	-
workspace:statistics:getMetric	Grants permission to query metrics.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:statistics:getMetricTrend	Grants permission to query the metric trend.	read	-	-
workspace:statistics:updateNotificationRules	Grants permission to update a metric notification rule.	write	-	-
workspace:statistics:deleteNotificationRules	Grants permission to delete a metric notification rule.	write	-	-
workspace:statistics:createNotifyRules	Grants permission to add a metric notification rule.	write	-	-
workspace:statistics:listNotificationRules	Grants permission to query metric notification rules.	list	-	-
workspace:statistics:listNotificationRecords	Grants permission to query metric notification records.	list	-	-
workspace:statistics:listDesktopMetrics	Grants permission to query desktop usage statistics.	list	-	-
workspace:statistics:exportDesktopMetrics	Grants permission to export desktop usage statistics.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:statistics:listUserMetrics	Grants permission to query user usage statistics.	list	-	-
workspace:statistics:exportUserMetrics	Grants permission to export user usage statistics.	list	-	-
workspace:appcenter:createBucketCredential	Grants permission to generate OBS bucket credential information.	write	-	-
workspace:appcenter:createAndAuthorizeBucket	Grants permission to add a default OBS bucket and access the bucket.	write	-	-
workspace:appcenter:listApps	Grants permission to query applications by name.	list	-	-
workspace:appcenter:createApp	Grants permission to upload an application.	write	-	-
workspace:appcenter:updateApp	Grants permission to modify an application.	write	-	-
workspace:appcenter:deleteApp	Grants permission to delete an application.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appcenter:installApp	Grants permission to automatically install an application.	write	-	-
workspace:appcenter:listAppAuthorizations	Grants permission to query application authorization information.	list	-	-
workspace:appcenter:batchUpdateAppAuthorizations	Grants permission to set application authorization.	write	-	-
workspace:appcenter:batchDeleteApps	Grants permission to delete applications in batches.	write	-	-
workspace:appcenter:batchDisableApps	Grants permission to set applications to be invisible in batches.	write	-	-
workspace:appcenter:batchEnableApps	Grants permission to set applications to be visible in batches.	write	-	-
workspace:appcenter:batchInstallApps	Grants permission to automatically install applications in batches.	write	-	-
workspace:appcenter:listAppCatalogs	Grants permission to query application categories.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appcenter:listJobs	Grants permission to query application installation job information.	list	-	-
workspace:appcenter:batchDeleteJobs	Grants permission to delete jobs in batches.	write	-	-
workspace:appcenter:retryJobs	Grants permission to retry a failed job.	write	-	-
workspace:appcenter:createAppRule	Grants permission to create an application rule.	write	-	-
workspace:appcenter:listAppRule	Grants permission to query application rules.	list	-	-
workspace:appcenter:updateAppRule	Grants permission to modify an application rule.	write	-	-
workspace:appcenter:deleteAppRule	Grants permission to delete an application rule.	write	-	-
workspace:appcenter:batchDeleteAppRules	Grants permission to delete application rules in batches.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appcenter:enableRuleRestriction	Grants permission to enable rule control.	write	-	-
workspace:appcenter:disableRuleRestriction	Grants permission to disable rule control.	write	-	-
workspace:appcenter:addRestrictedRule	Grants permission to add a control rule.	write	-	-
workspace:appcenter:listRestrictedRule	Grants permission to query control rules.	list	-	-
workspace:appcenter:deleteRestrictedRule	Grants permission to delete control rules in batches.	write	-	-
workspace:appcenter:updateTenantProfile	Grants permission to enable or disable the tenant function.	write	-	-
workspace:appcenter:listTenantProfiles	Grants permission to query the tenant function status.	list	-	-
workspace:scripts:create	Grants permission to create a script.	write	script *	-
workspace:scripts:list	Grants permission to query the script list.	list	script *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:scripts:get	Grants permission to query script details.	read	script *	-
workspace:scripts:put	Grants permission to update a script.	write	script *	-
workspace:scripts:delete	Grants permission to delete a script.	write	script *	-
workspace:scripts:execute	Grants permission to run scripts or commands in batches.	write	script *	-
			desktop *	-
workspace:scripts:getRecordDetail	Grants permission to query script or command execution record details.	read	script *	-
workspace:scripts:listRecords	Grants permission to query script execution records.	list	script *	-
workspace:scripts:listTasks	Grants permission to query script tasks.	list	script *	-
workspace:scripts:retry	Grants permission to retry a script.	write	script *	-
workspace:scripts:stop	Grants permission to stop a script or command execution task.	write	script *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:scripts:download	Grants permission to download a script output record.	write	script *	-
workspace:tenants:getShareSpaceConfig	Grants permission to query collaboration configurations.	read	-	-
workspace:tenants:updateShareSpaceConfig	Grants permission to modify collaboration configurations.	write	-	-
workspace:authConfigs:getStatus	Grants permission to query the authentication status.	read	-	-
workspace:privacystatements:sign	Grants permission to sign the privacy statement.	write	-	-
workspace:sites:get	Grants permission to query site information.	read	-	-
workspace:sites:add	Grants permission to add a site.	write	-	workspace:AccessMode
workspace:sites:delete	Grants permission to delete a site.	write	-	-
workspace:sites:updateAccessMode	Grants permission to change the site access mode.	write	-	workspace:AccessMode

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:sites:updateSubnets	Grants permission to change the site service subnet.	write	-	-
workspace:tenants:checkEnterpriseIds	Grants permission to check whether the enterprise ID has been used.	write	-	-
workspace:tenants:updateEnterpriseId	Grants permission to change the enterprise ID.	write	-	-
workspace:bandwidth:create	Grants permission to enable the Workspace bandwidth.	write	-	-
workspace:bandwidth:list	Grants permission to query the Workspace bandwidth list.	list	-	-
workspace:bandwidth:update	Grants permission to modify the Workspace bandwidth.	write	-	-
workspace:bandwidth:delete	Grants permission to cancel the Workspace bandwidth.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:bandwidth:getControlConfig	Grants permission to query the control configuration of the Workspace bandwidth.	read	-	-
workspace:bandwidth:updateControlConfig	Grants permission to modify the control configuration of the Workspace bandwidth.	write	-	-
workspace:bandwidth:createChangeOrder	Grants permission to create a Workspace bandwidth change order.	write	-	-
workspace:desktops:batchCreateSnapshots	Grants permission to create desktop snapshots in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDeleteSnapshots	Grants permission to delete desktop snapshots in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchRestoreSnapshots	Grants permission to restore desktop snapshots in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listSnapshots	Grants permission to query desktop snapshots.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:verifyDesktopName	Grants permission to verify the desktop name.	write	-	-
workspace:networks:getAvailableIp	Grants permission to query available IP addresses of a subnet by subnet ID.	read	-	-
workspace:desktops:getAdStatus	Grants permission to query the AD network status.	read	-	-
workspace:networks:checkIpIfExist	Grants permission to check whether the IP address exists.	write	-	-
workspace:images:checkIfExist	Grants permission to check whether the image exists.	write	-	-
workspace:wdh:listDesktops	Grants permission to query desktops of a Workspace host.	list	wdh *	-
			-	g:EnterpriseProjectId
workspace:wdh:update	Grants permission to update Workspace host information.	write	wdh *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:bindingPolicies:getTemplate	Grants permission to download the template for terminal-desktop binding.	read	-	-
workspace:bindingPolicies:import	Grants permission to import terminal-desktop binding in batches.	write	-	-
workspace:statistics:getRunState	Grants permission to collect statistics on running statuses.	read	-	-
workspace:statistics:getLoginState	Grants permission to collect statistics on login statuses.	read	-	-
workspace:networks:getUsingSubnets	Grants permission to query subnets being used.	read	-	-
workspace:networks:listPorts	Grants permission to query ports.	list	-	-
workspace:renderDesktops:createConsole	Grants permission to obtain the URL for remote login to the console.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:renderDesktops:resize	Grants permission to change rendering desktop specifications.	write	-	-
workspace:exclusiveHosts:resizeLites	Grants permission to modify exclusive host specifications.	write	exclusiveHost *	g:EnterpriseProjectId
workspace:desktops:getMonitor	Grants permission to query desktop monitoring information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetachInfo	Grants permission to query users unbound from the desktop.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:getSysprepVersion	Grants permission to query Sysprep version information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:networks:createNat	Grants permission to enable the Internet access function of the NAT Gateway.	write	-	-
workspace:networks:listNats	Grants permission to query the Internet access function of the NAT Gateway.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:networks:listSubnets	Grants permission to query subnets.	list	-	-
workspace:networks:listVpcs	Grants permission to query VPCs.	list	-	-
workspace:policyGroups:createTemplate	Grants permission to create a policy template.	write	-	-
workspace:policyGroups:listTemplate	Grants permission to query policy templates.	list	-	-
workspace:policyGroups:updateTemplate	Grants permission to update a policy template.	write	-	-
workspace:networks:listSecurityGroups	Grants permission to query security groups.	list	-	-
workspace:availabilityZones:getSummary	Grants permission to query AZ summary.	read	-	-
workspace:availabilityZones:get	Grants permission to query AZ details.	read	-	-
workspace:users:importUser	Grants permission to import a user list.	write	user *	-
workspace:users:uploadTemplate	Grants permission to import a desktop user list.	write	user *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:accessPolicies:update	Grants permission to update a specified access policy.	write	-	-
workspace:desktops:verifySource	Grants permission to verify desktop sources.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDesktopNetworks	Grants permission to query desktop network information in batches.	list	desktop *	-
workspace:desktops:batchChangeNetwork	Grants permission to switch desktop networks in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:get	Grants permission to query task details.	read	-	-
workspace:accessPolicies:importIp	Grants permission to import the IP address list.	write	-	-
workspace:accessPolicies:getIpImportTemplate	Grants permission to download the template for importing IP addresses.	read	-	-
workspace:sites:listEdgeSites	Grants permission to query edge sites.	list	-	-
workspace:sites:checkEdgeSiteResources	Grants permission to verify edge site resources.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:ou:listAdOus	Grants permission to query OU information in the AD domain.	list	-	-
workspace:ou:listOuUsers	Grants permission to query user information in the OU.	list	-	-
workspace:ou:importUsersByOU	Grants permission to import OU users.	write	-	-
workspace:appGroup:list	Grants permission to query application groups.	list	appGroup *	-
workspace:appGroup:create	Grants permission to create an application group.	write	appGroup *	-
			serverGroup	-
workspace:appGroup:delete	Grants permission to delete an application group.	write	appGroup *	-
workspace:appGroup:get	Grants permission to query application group details.	read	appGroup *	-
workspace:appGroup:update	Grants permission to modify an application group.	write	appGroup *	-
			serverGroup	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:app:listPublishedApp	Grants permission to query published applications.	list	app *	-
			appGroup *	-
workspace:app:publish	Grants permission to publish an application.	write	app *	-
			appGroup *	-
workspace:app:get	Grants permission to query application details.	read	app *	-
			appGroup *	-
workspace:app:update	Grants permission to modify application information.	write	app *	-
			appGroup *	-
workspace:app:deleteIcon	Grants permission to delete a custom application icon.	write	app *	-
			appGroup *	-
workspace:app:uploadIcon	Grants permission to modify a custom application icon.	write	app *	-
			appGroup *	-
workspace:app:check	Grants permission to verify applications.	write	app *	-
			appGroup *	-
workspace:app:batchDisable	Grants permission to disable applications in batches.	write	app *	-
			appGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:app:batchEnable	Grants permission to enable applications in batches.	write	app *	-
			appGroup *	-
workspace:app:unpublish	Grants permission to unpublish applications in batches.	write	app *	-
			appGroup *	-
workspace:appGroup:listPublishableApp	Grants permission to query applications that can be published.	list	appGroup *	-
workspace:appGroup:batchDeleteAuthorization	Grants permission to remove application group authorization.	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:disassociate	Grants permission to disassociate a service group from all application groups.	write	-	-
workspace:appGroup:listAuthorization	Grants permission to query application group authorization records.	list	appGroup *	-
workspace:appGroup:addAuthorization	Grants permission to add application group authorization.	write	appGroup *	-
			user	-
			userGroup	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appGroup:batchDelete	Grants permission to delete application groups in batches.	write	appGroup *	-
workspace:appGroup:check	Grants permission to verify an application group.	write	-	-
workspace:serverGroup:list	Grants permission to query server groups.	list	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:create	Grants permission to create a server group.	write	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:delete	Grants permission to delete a server group.	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:get	Grants permission to query a specified server group.	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:update	Grants permission to modify a server group.	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:serverGroup:getServerState	Grants permission to query server statuses in a specified server group.	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:listDetail	Grants permission to query basic information about a tenant server group.	list	serverGroup *	-
workspace:serverGroup:getRestrict	Grants permission to query specified tenant server groups.	read	serverGroup *	-
workspace:serverGroup:validate	Grants permission to verify a server group.	write	serverGroup *	-
workspace:serverGroup:tagResource	Grants permission to add a tag to a server group.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:unTagResource	Grants permission to delete a tag from a server group.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:listTagsForResource	Grants permission to query server group tags.	list	serverGroup *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:serverGroup:listTags	Grants permission to query tags on all servers of a tenant.	list	serverGroup *	-
workspace:serverGroup:batchCreateTags	Grants permission to add server group tags in batches.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:batchDeleteTags	Grants permission to delete server group tags in batches.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:server:list	Grants permission to query servers.	list	server *	-
workspace:server:delete	Grants permission to delete a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:get	Grants permission to query a specified server.	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:update	Grants permission to modify a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:changeImage	Grants permission to modify a server image.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:server:reinstall	Grants permission to reinstall a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:getVncUrl	Grants permission to obtain a VNC login address.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:list	Grants permission to query the latest versions of all HDAs of a tenant.	list	-	-
workspace:accessAgent:batchUpgrade	Grants permission to upgrade the HDA version of servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:listLatestVersion	Grants permission to query the latest HDA version of a tenant.	list	-	-
workspace:server:listAccessAgentDetails	Grants permission to query HDA information of a server.	list	server *	-
workspace:accessAgent:getUpgradeFlag	Grants permission to query HDA upgrade notification flags.	read	-	-
workspace:accessAgent:updateUpgradeFlag	Grants permission to update an HDA upgrade notification flag.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:accessAgent:listUpgradeRecords	Grants permission to query HDA upgrade tracing records of a server.	list	-	-
workspace:server:batchDelete	Grants permission to delete servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchChangeMaintainMode	Grants permission to mark the server maintenance status.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReboot	Grants permission to restart a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchRejoinDomain	Grants permission to add servers to a domain again in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStart	Grants permission to start a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStop	Grants permission to stop a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchUpdateTsvi	Grants permission to update virtual session IP configurations of servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:server:create	Grants permission to create an APS.	write	server *	-
			serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:server:batchMigrateHosts	Grants permission to migrate servers at the source Workspace host to the destination one.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			wdh *	-
workspace:server:getMetricData	Grants permission to query monitoring information of an APS.	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:batchDeleteSubJobs	Grants permission to delete subtasks in batches.	write	-	-
workspace:jobs:countSubJobs	Grants permission to query the number of subtasks.	list	-	-
workspace:appWarehouse:authorizeObs	Grants permission to obtain the AK/SK uploaded to an OBS bucket.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appWarehouse:batchDeleteApp	Grants permission to delete specified applications from the application repository in batches.	write	-	-
workspace:appWarehouse:ListWarehouseApps	Grants permission to query applications in a tenant application repository.	list	-	-
workspace:appWarehouse:createApp	Grants permission to add an application to the application repository.	write	-	-
workspace:appWarehouse:deleteApp	Grants permission to delete a specified application from the application repository.	write	-	-
workspace:appWarehouse:uploadAppIcon	Grants permission to upload an icon file to the application repository.	write	-	-
workspace:appWarehouse:createBucketOrAcl	Grants permission to add a bucket or authorize access to a bucket.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:images:listImageJobs	Grants permission to query tasks of a tenant.	list	-	-
workspace:images:getImageJob	Grants permission to query task details.	read	-	-
workspace:imageServer:list	Grants permission to query image instances.	list	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:create	Grants permission to create an image instance.	write	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:get	Grants permission to query a specified image instance.	read	imageServer *	g:EnterpriseProjectId
workspace:imageServer:update	Grants permission to modify an image instance.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:attachApp	Grants permission to distribute software information to image instances.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listLatestAttachedApp	Grants permission to query information about the latest distributed software.	list	imageServer *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:imageServer:recreate	Grants permission to build an Application Streaming image.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:batchDelete	Grants permission to delete image instances in batches.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listImageSubJobs	Grants permission to query subtasks.	list	-	-
workspace:imageServer:batchDeleteImageSubJobs	Grants permission to delete subtasks in batches.	write	-	-
workspace:imageServer:countImageSubJobs	Grants permission to query the number of subtasks.	read	-	-
workspace:appGroup:listMailRecord	Grants permission to query records of sending emails on application group authorization.	list	-	-
workspace:appGroup:resendMail	Grants permission to resend an email on application group authorization (based on authorization email records).	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:storage:listPersistentStorage	Grants permission to query Workspace storage space.	list	storage *	-
workspace:storage:createPersistentStorage	Grants permission to create Workspace storage space.	write	storage *	-
workspace:storage:deletePersistentStorage	Grants permission to delete Workspace storage space.	write	storage *	-
workspace:storage:updateUserFolderAssignment	Grants permission to create a personal storage directory.	write	storage *	-
workspace:storage:updateShareFolderAssignment	Grants permission to change members of a shared directory.	write	storage *	-
workspace:storage:createShareFolder	Grants permission to create a shared storage directory.	write	storage *	-
workspace:storage:deleteStorageClaim	Grants permission to delete a shared directory.	write	storage *	-
workspace:storage:deleteUserStorageAttachment	Grants permission to delete a personal storage directory.	write	storage *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:storage:batchDeletePersistentStorage	Grants permission to delete Workspace storage space in batches.	write	storage *	-
workspace:storage:listStorageAssignment	Grants permission to query personal storage directories.	list	storage *	-
workspace:storage:listShareFolder	Grants permission to query shared storage directories.	list	storage *	-
workspace:policyGroups:deleteTemplate	Grants permission to delete a policy template.	write	-	-
workspace:privacystatements:get	Grants permission to query the latest privacy statement.	read	-	-
workspace:scalingPolicy:delete	Grants permission to delete an auto scaling policy.	write	-	-
workspace:scalingPolicy:list	Grants permission to query auto scaling policies of a server group.	read	-	-
workspace:scalingPolicy:create	Grants permission to add or modify an auto scaling policy.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:session:listAppConnection	Grants permission to query application usage records.	write	-	-
workspace:session:logoffUserSession	Grants permission to log out of a session.	write	-	-
workspace:session:listUserConnection	Grants permission to query user login records.	write	-	-
workspace:session:listSessionByUserName	Grants permission to query current sessions by username.	list	-	-
workspace:storagePolicy:create	Grants permission to add or update a custom policy for storage directory access.	write	storage *	-
workspace:storagePolicy:list	Grants permission to query policies for storage directory access.	list	storage *	-
workspace:storage:listSfs3Storage	Grants permission to query SFS 3.0.	list	storage *	-
workspace:baseResource:list	Grants permission to query AZs.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:tenants:listConfigInfo	Grants permission to query enterprise system configurations.	list	-	-
workspace:tenants:active	Grants permission to activate and initialize a tenant service.	write	-	-
workspace:tenants:listTenantProfile	Grants permission to query tenant information.	list	-	-
workspace:server:listServerMetricData	Grants permission to query server monitoring data.	list	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:session:listSessions	Grants permission to query enterprise sessions.	list	-	-
workspace:appWarehouse:updateApp	Grants permission to update an application in the application repository.	write	-	-
workspace:server:batchChangeImage	Grants permission to switch server images in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReinstall	Grants permission to reinstall servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:authConfigs:get	Grants permission to query the configuration of the authentication login mode.	read	-	-
workspace:authConfigs:update	Grants permission to update authentication policy configurations.	write	-	-
workspace:assistAuthConfigs:get	Grants permission to query auxiliary authentication configurations.	read	-	-
workspace:assistAuthConfigs:update	Grants permission to update auxiliary authentication configurations.	write	-	-
workspace:jobs:retry	Grants permission to retry a task.	write	-	-
workspace:quotas:get	Grants permission to query tenant quotas.	read	-	-
workspace:tenants:getRoles	Grants permission to query tenant roles.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:tenants:ListConfig	Grants permission to query customized tenant configurations.	list	-	-
workspace:tenants:updateConfig	Grants permission to modify customized tenant configurations.	write	-	-
workspace:natMappings:getConfig	Grants permission to query NAT mapping configuration items of a tenant.	read	-	-
workspace:natMappings:updateConfig	Grants permission to modify NAT mapping configuration items of a tenant.	write	-	-
workspace:tenants:get	Grants permission to query Huawei Cloud Workspace details.	read	-	-
workspace:tenants:open	Grants permission to subscribe to Huawei Cloud Workspace.	write	-	workspace:AccessMode

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:tenants:delete	Grants permission to unsubscribe from Huawei Cloud Workspace.	write	-	-
workspace:tenants:update	Grants permission to modify attributes of Huawei Cloud Workspace.	write	-	workspace:AccessMode
workspace:tenants:getLockStatus	Grants permission to query whether Huawei Cloud Workspace is locked.	read	-	-
workspace:tenants:unlock	Grants permission to unlock Huawei Cloud Workspace.	write	-	-
workspace:agencies:create	Grants permission to create an agency.	write	-	-
workspace:agencies:get	Grants permission to query agencies.	read	-	-
workspace:desktops:commitAiAccelerateJob	Grants permission to create a rendering acceleration task.	write	-	-
workspace:desktops:getAiAccelerateJob	Grants permission to query rendering acceleration tasks.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:getSysPrepInfo	Grants permission to query Sysprep details.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:checkBatchChangeImage	Grants permission to verify batch image switchover.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:tenants:listDesktopNamePolicies	Grants permission to query desktop naming policies.	list	-	-
workspace:tenants:createDesktopNamePolicy	Grants permission to create a desktop naming policy.	write	-	-
workspace:tenants:updateDesktopNamePolicy	Grants permission to update a desktop naming policy.	write	-	-
workspace:tenants:batchDeleteDesktopNamePolicies	Grants permission to delete desktop naming policies in batches.	write	-	-
workspace:desktopPools:create	Grants permission to create a desktop pool.	write	desktopPool *	-
			user	-
			userGroup	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktopPools:list	Grants permission to query desktop pools.	list	desktopPool *	-
workspace:desktopPools:update	Grants permission to modify desktop pool attributes.	write	desktopPool *	-
workspace:desktopPools:delete	Grants permission to delete a desktop pool.	write	desktopPool *	-
workspace:desktopPools:get	Grants permission to query desktop pool details.	read	desktopPool *	-
workspace:desktopPools:expand	Grants permission to expand the desktop pool capacity.	write	desktopPool *	-
workspace:desktopPools:resize	Grants permission to change desktop pool specifications.	write	desktopPool *	-
workspace:desktopPools:rebuild	Grants permission to recompose the system disk of a desktop pool.	write	desktopPool *	-
workspace:desktopPools:batchAddVolumes	Grants permission to add disks to desktop pools in batches.	write	desktopPool *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktopPools:batchDeleteVolumes	Grants permission to delete disks from desktop pools in batches.	write	desktopPool *	-
workspace:desktopPools:batchExpandVolumes	Grants permission to expand the capacity of disks in batches in a desktop pool.	write	desktopPool *	-
workspace:desktopPools:operate	Grants permission to perform operations on a desktop pool.	write	desktopPool *	-
workspace:desktopPools:listUsers	Grants permission to query users and user groups authorized by the desktop pool.	list	desktopPool *	-
workspace:desktopPools:authorizeUsers	Grants permission to authorize users and user groups to access a desktop pool.	write	desktopPool *	-
			user	-
			userGroup	-
workspace:desktopPools:listDesktops	Grants permission to query desktop information in desktop pools.	list	desktopPool *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktopPools:listScriptTasks	Grants permission to query the script execution task list of a desktop pool.	list	desktopPool *	-
workspace:desktopPools:executeScripts	Grants permission to execute desktop pool scripts in batches.	write	desktopPool *	-
			script	-
workspace:desktopPools:sendNotifications	Grants permission to send notifications.	write	desktopPool *	-
workspace:desktops:export	Grants permission to export a desktop list.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:create	Grants permission to create a desktop.	write	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId • workspace:AssociatePublicIp • workspace:AccessMode
workspace:desktops:list	Grants permission to query desktops.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:update	Grants permission to update desktop information.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:delete	Grants permission to delete a desktop.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:get	Grants permission to query desktop details.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDelete	Grants permission to delete desktops in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:logoff	Grants permission to log out of desktops in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetail	Grants permission to query desktop details.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:operate	Grants permission to perform operations on a desktop.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:resize	Grants permission to change specifications.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:getConnectStatus	Grants permission to query desktop login status statistics.	read	-	-
workspace:desktops:ListStatus	Grants permission to query desktop login statuses.	list	-	-
workspace:desktops:rebuild	Grants permission to recompose desktops.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getActions	Grants permission to query desktop power-on/off information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createConsole	Grants permission to obtain the URL for remote login to the console.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:updateSids	Grants permission to update a desktop SID.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:rejoinDomain	Grants permission to rejoin the AD domain.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createImage	Grants permission to convert a desktop to an image.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDetach	Grants permission to unbind users in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:detach	Grants permission to unbind a user.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:attach	Grants permission to assign a desktop to a user.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getNetwork	Grants permission to query desktop network information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeNetwork	Grants permission to switch the desktop network.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:exclusiveHosts:listDesktops	Grants permission to query exclusive desktop details.	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:desktops:listAll	Grants permission to query general-purpose desktops and rendering desktops.	list	desktop *	-
workspace:desktopAssociate:listDiscoverVmInfo	Grants permission to query the list of VMs that can be managed.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktopAssociate:startTask	Grants permission to start a VM management task.	write	-	-
workspace:desktopAssociate:switchScanTask	Grants permission to enable a management scanning task.	write	-	-
workspace:desktopAssociate:getScanTaskSwitch	Grants permission to query management scanning tasks.	read	-	-
workspace:desktops:setMaintenanceMode	Grants permission to set the desktop administrator maintenance mode in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:prepAttachUsers	Grants permission to pre-assign desktops to users in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchAttachUsers	Grants permission to assign desktops to users in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:changeUsername	Grants permission to change usernames associated with desktops in Windows AD.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:sendNotifications	Grants permission to send notifications.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:migrate	Grants permission to migrate desktops.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listAgents	Grants permission to query the list of desktops with installed agents.	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchInstallAgents	Grants permission to install agents for desktops in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listTags	Grants permission to query desktop tags.	list	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:tag	Grants permission to create a desktop tag.	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:untag	Grants permission to delete a desktop tag.	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:listProjectTags	Grants permission to query project tags.	list	-	-
workspace:desktops:operateTags	Grants permission to add or delete tags in batches.	tagging	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:desktops:listByTags	Grants permission to filter desktops by tag.	list	-	-
workspace:exclusiveHosts:create	Grants permission to create an exclusive host.	write	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:list	Grants permission to query exclusive hosts.	list	exclusiveHost *	-
			-	g:EnterpriseProjectId
workspace:exclusiveHosts:check	Grants permission to check whether exclusive hosts can be created.	write	-	-
workspace:exclusiveHosts:get	Grants permission to query exclusive host details.	read	exclusiveHost *	g:EnterpriseProjectId
workspace:exclusiveHosts:update	Grants permission to update exclusive host information.	write	exclusiveHost *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:exclusiveHosts:delete	Grants permission to delete an exclusive host.	write	exclusiveHost *	g:EnterpriseProjectId
workspace:mkp:listImages	Grants permission to query images in KooGallery.	list	-	-
workspace:mkp:listCommodityInfos	Grants permission to query product information in KooGallery.	list	-	-
workspace:mkp:createOrder	Grants permission to create a product order in KooGallery.	write	-	-
workspace:mkp:listListProductReserve	Grants permission to query the KooGallery inventory.	list	-	-
workspace:mkp:listCommodityDetails	Grants permission to query product details in KooGallery.	list	-	-
workspace:mkp:listRelationCommodityDetails	Grants permission to query associated products.	list	-	-
workspace:mkp:listCommodityAgreements	Grants permission to query product agreements in KooGallery.	list	-	-
workspace:networks:listEips	Grants permission to query EIPs.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:networks:createEips	Grants permission to create an EIP.	write	-	-
workspace:networks:bindEips	Grants permission to bind an EIP.	write	-	-
workspace:networks:unbindEips	Grants permission to unbind an EIP.	write	-	-
workspace:networks:getEipQuota	Grants permission to query EIP quotas.	read	-	-
workspace:networks:ListNatGateways	Grants permission to query NAT gateways.	list	-	-
workspace:orders:create	Grants permission to place a yearly/monthly order.	write	-	• workspace:CreateOrderType • workspace:AssociatePublicIp • workspace:AccessMode
workspace:orders:change	Grants permission to create a change order.	write	-	workspace:ChangeOrderType
workspace:orders:batchInquiry	Grants permission to inquire prices in batches.	write	-	-
workspace:quotas:check	Grants permission to verify quotas.	write	-	-
workspace:renderDesktops:create	Grants permission to create a rendering desktop.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:renderDesktops:delete	Grants permission to delete a rendering desktop.	write	-	-
workspace:renderDesktops:list	Grants permission to query rendering desktops.	list	-	-
workspace:renderDesktops:action	Grants permission to perform operations on a rendering desktop.	write	-	-
workspace:scheduledTasks:list	Grants permission to query scheduled tasks.	list	scheduledTask *	-
workspace:scheduledTasks:create	Grants permission to create a scheduled task.	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-
workspace:scheduledTasks:get	Grants permission to query scheduled task details.	read	scheduledTask *	-
workspace:scheduledTasks:update	Grants permission to update a scheduled task.	write	scheduledTask *	-
			desktop	-
			desktopPool	-
			server	-
			serverGroup	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:scheduledTasks:delete	Grants permission to delete a scheduled task.	write	scheduledTask *	-
workspace:scheduledTasks:getFuture	Grants permission to query the future execution time of a scheduled task.	read	-	-
workspace:scheduledTasks:batchDelete	Grants permission to delete scheduled tasks in batches.	write	scheduledTask *	-
workspace:scheduledTasks:listRecords	Grants permission to query the execution records of a scheduled task.	list	scheduledTask *	-
workspace:scheduledTasks:getRecord	Grants permission to query details about scheduled task execution records.	read	scheduledTask *	-
workspace:scheduledTasks:exportRecords	Grants permission to export details about scheduled task execution records.	list	scheduledTask *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:subscribeSharer	Grants permission to subscribe to collaborative resources.	write	user *	-
workspace:desktops:addSubResources	Grants permission to purchase depended desktop resources.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSubResources	Grants permission to delete depended desktop resources.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createSnapshots	Grants permission to create a desktop snapshot.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:getSnapshots	Grants permission to query desktop snapshots.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:deleteSnapshots	Grants permission to delete a desktop snapshot.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:restoreBySnapshot	Grants permission to restore desktops using desktop snapshots.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:statistics:listDesktopStatus	Grants permission to collect statistics on desktop statuses.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:statistics:getUnused	Grants permission to query desktops that are not in use in a specified period.	read	-	-
workspace:statistics:getUsed	Grants permission to query the desktop usage duration.	read	-	-
workspace:bindingPolicies:export	Grants permission to export information about terminal-desktop binding to an Excel file.	list	-	-
workspace:bindingPolicies:getConfig	Grants permission to query a terminal-desktop binding configuration.	read	-	-
workspace:bindingPolicies:createConfig	Grants permission to configure terminal-desktop binding.	write	-	-
workspace:bindingPolicies:get	Grants permission to query terminal-desktop binding configurations.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:bindingPolicies:add	Grants permission to add a terminal-desktop binding configuration.	write	-	-
workspace:bindingPolicies:update	Grants permission to modify a terminal-desktop binding configuration.	write	-	-
workspace:bindingPolicies:delete	Grants permission to delete a terminal-desktop binding configuration.	write	-	-
workspace:volumes:delete	Grants permission to delete a desktop data disk.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchAdd	Grants permission to add a desktop disk.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:batchExpand	Grants permission to expand a desktop disk.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:wdh:getType	Grants permission to query Workspace host types.	read	wdh *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:wdh:get	Grants permission to query Workspace hosts.	read	wdh *	g:EnterpriseProjectId
workspace:desktops:getRemoteAssistance	Grants permission to query remote assistance information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:createRemoteAssistance	Grants permission to create remote assistance.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:cancelRemoteAssistance	Grants permission to cancel remote assistance.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:add	Grants permission to add disks to a single desktop.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:expand	Grants permission to expand disk capacity.	write	desktop	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:volumes:listDssPoolsDetail	Grants permission to obtain the dedicated distributed storage pool list.	list	-	-
workspace:common:listTimezones	Grants permission to query the time zone configuration.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:connections:securityExport	Grants permission to export connection records.	list	-	-
workspace:images:list	Grants permission to query supported images.	list	-	-
workspace:policyGroups:import	Grants permission to import a policy group.	write	-	-
workspace:accessPolicies:create	Grants permission to create an access policy.	write	-	-
workspace:accessPolicies:get	Grants permission to query access policies.	read	-	-
workspace:accessPolicies:delete	Grants permission to delete a specified access policy.	write	-	-
workspace:accessPolicies:getTarget	Grants permission to query objects to which a specified access policy is applied.	read	-	-
workspace:accessPolicies:updateTarget	Grants permission to update objects to which a specified access policy is applied.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:products:listDesktopProducts	Grants permission to query the list of available product packages.	list	-	-
workspace:products:listSharerProducts	Grants permission to query the list of collaboration packages.	list	-	-
workspace:products:listInternetProducts	Grants permission to query the list of Internet access packages.	list	-	-
workspace:availabilityZones:list	Grants permission to query AZs where Workspace is available.	list	-	-
workspace:userGroups:export	Grants permission to export a user group.	list	userGroup *	-
workspace:users:export	Grants permission to export a user.	list	user *	-
workspace:users:import	Grants permission to import a user.	write	user *	-
workspace:userGroups:exportUsers	Grants permission to export users in a user group.	list	userGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:operate	Grants permission to operators (locking, unlocking, and resetting passwords).	write	user *	-
workspace:users:randomPassword	Grants permission to reset a random password for a user.	write	user *	-
workspace:users:deleteOtps	Grants permission to unbind an OTP device.	write	user *	-
workspace:users:resendEmail	Grants permission to resend an email.	write	user *	-
workspace:connections:securityList	Grants permission to query connection information.	list	-	-
workspace:connections:listOnlineUsers	Grants permission to query the number of login users.	list	-	-
workspace:userGroups:list	Grants permission to query user groups.	list	userGroup *	-
workspace:userGroups:create	Grants permission to create a user group.	write	userGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:userGroups:batchDelete	Grants permission to delete user groups in batches.	write	userGroup *	-
workspace:userGroups:delete	Grants permission to delete a desktop user group.	write	userGroup *	-
workspace:userGroups:update	Grants permission to modify user group information.	write	userGroup *	-
workspace:userGroups:operate	Grants permission to perform operations on a user group.	write	userGroup *	-
			user *	-
workspace:userGroups:getUsers	Grants permission to query users in a user group.	list	userGroup *	-
workspace:jobs:listSubJobs	Grants permission to query subtasks.	list	-	-
workspace:jobs:deleteSubJobRecords	Grants permission to delete a subtask record.	write	-	-
workspace:ou:get	Grants permission to query OU information.	list	-	-
workspace:ou:create	Grants permission to add OU information.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:ou:delete	Grants permission to delete OU information.	write	-	-
workspace:ou:update	Grants permission to update OU information.	write	-	-
workspace:policyGroups:list	Grants permission to query policy groups.	list	policyGroup *	-
workspace:policyGroups:create	Grants permission to add a policy group.	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:delete	Grants permission to delete a policy group.	write	policyGroup *	-
workspace:policyGroups:get	Grants permission to query policy groups.	read	policyGroup *	-
workspace:policyGroups:update	Grants permission to modify a policy group.	write	policyGroup *	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:export	Grants permission to export a policy group.	list	policyGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:policyGroups:listPolicies	Grants permission to query policy items of a policy group.	list	policyGroup *	-
workspace:policyGroups:updatePolicies	Grants permission to modify policy items of a policy group.	write	policyGroup *	-
workspace:policyGroups:listTargets	Grants permission to query objects to which the policy group is applied.	list	policyGroup *	-
workspace:policyGroups:updateTargets	Grants permission to modify objects to which the policy group is applied.	write	policyGroup *	-
			desktop	-
			desktopPool	-
			user	-
			userGroup	-
			appGroup	-
workspace:policyGroups:listDetail	Grants permission to query details about policy groups.	list	policyGroup *	-
workspace:policyGroups:getOriginalPolicies	Grants permission to query initial policy items.	read	policyGroup *	-
workspace:users:list	Grants permission to query users.	list	user *	-
workspace:users:create	Grants permission to create a user.	write	user *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:delete	Grants permission to delete a specified user.	write	user *	-
workspace:users:get	Grants permission to query user details.	read	user *	-
workspace:users:update	Grants permission to modify user information.	write	user *	-
workspace:users:batchDelete	Grants permission to delete users in batches.	write	user *	-
workspace:users:resetPassword	Grants permission to reset a user password.	write	user *	-
workspace:users:checkResetPasswordToken	Grants permission to verify tokens for resetting passwords of domain users.	write	user *	-
workspace:users:getTemplate	Grants permission to download a user template.	read	-	-
workspace:users:checkExist	Grants permission to check whether the user exists.	write	user *	-
workspace:users:listOtps	Grants permission to query OTP devices.	list	user *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:users:getImportTemplate	Grants permission to download a created user template.	read	-	-
workspace:users:batchCreate	Grants permission to create users in batches.	write	user *	-
workspace:products:listVolumeProducts	Grants permission to query disk products.	list	-	-
workspace:tenants:listExportTasks	Grants permission to query export tasks.	list	-	-
workspace:tenants:deleteExportTasks	Grants permission to delete export task records in batches.	write	-	-
workspace:tenants:exportData	Grants permission to download an exported file.	read	-	-
workspace:statistics:listAlarm	Grants permission to query alarms.	list	-	-
workspace:statistics:getAlarm	Grants permission to query the number of alarms.	read	-	-
workspace:statistics:getGrowthRate	Grants permission to query the chain value of a metric.	read	-	-
workspace:statistics:getMetric	Grants permission to query metrics.	read	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:statistics:getMetricTrend	Grants permission to query the metric trend.	read	-	-
workspace:statistics:updateNotificationRules	Grants permission to update a metric notification rule.	write	-	-
workspace:statistics:deleteNotificationRules	Grants permission to delete a metric notification rule.	write	-	-
workspace:statistics:createNotifyRules	Grants permission to add a metric notification rule.	write	-	-
workspace:statistics:listNotificationRules	Grants permission to query metric notification rules.	list	-	-
workspace:statistics:listNotificationRecords	Grants permission to query metric notification records.	list	-	-
workspace:statistics:listDesktopMetrics	Grants permission to query desktop usage statistics.	list	-	-
workspace:statistics:exportDesktopMetrics	Grants permission to export desktop usage statistics.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:statistics:listUserMetrics	Grants permission to query user usage statistics.	list	-	-
workspace:statistics:exportUserMetrics	Grants permission to export user usage statistics.	list	-	-
workspace:appcenter:createBucketCredential	Grants permission to generate OBS bucket credential information.	write	-	-
workspace:appcenter:createAndAuthorizeBucket	Grants permission to add a default OBS bucket and access the bucket.	write	-	-
workspace:appcenter:listApps	Grants permission to query applications by name.	list	-	-
workspace:appcenter:createApp	Grants permission to upload an application.	write	-	-
workspace:appcenter:updateApp	Grants permission to modify an application.	write	-	-
workspace:appcenter:deleteApp	Grants permission to delete an application.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appcenter:installApp	Grants permission to automatically install an application.	write	-	-
workspace:appcenter:listAppAuthorizations	Grants permission to query application authorization information.	list	-	-
workspace:appcenter:batchUpdateAppAuthorizations	Grants permission to set application authorization.	write	-	-
workspace:appcenter:batchDeleteApps	Grants permission to delete applications in batches.	write	-	-
workspace:appcenter:batchDisableApps	Grants permission to set applications to be invisible in batches.	write	-	-
workspace:appcenter:batchEnableApps	Grants permission to set applications to be visible in batches.	write	-	-
workspace:appcenter:batchInstallApps	Grants permission to automatically install applications in batches.	write	-	-
workspace:appcenter:listAppCatalogs	Grants permission to query application categories.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appcenter:listJobs	Grants permission to query application installation job information.	list	-	-
workspace:appcenter:batchDeleteJobs	Grants permission to delete jobs in batches.	write	-	-
workspace:appcenter:retryJobs	Grants permission to retry a failed job.	write	-	-
workspace:appcenter:createAppRule	Grants permission to create an application rule.	write	-	-
workspace:appcenter:listAppRule	Grants permission to query application rules.	list	-	-
workspace:appcenter:updateAppRule	Grants permission to modify an application rule.	write	-	-
workspace:appcenter:deleteAppRule	Grants permission to delete an application rule.	write	-	-
workspace:appcenter:batchDeleteAppRules	Grants permission to delete application rules in batches.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appcenter:enableRuleRestriction	Grants permission to enable rule control.	write	-	-
workspace:appcenter:disableRuleRestriction	Grants permission to disable rule control.	write	-	-
workspace:appcenter:addRestrictedRule	Grants permission to add a control rule.	write	-	-
workspace:appcenter:listRestrictedRule	Grants permission to query control rules.	list	-	-
workspace:appcenter:deleteRestrictedRule	Grants permission to delete control rules in batches.	write	-	-
workspace:appcenter:updateTenantProfile	Grants permission to disable the tenant function.	write	-	-
workspace:appcenter:listTenantProfiles	Grants permission to query the tenant function status.	list	-	-
workspace:scripts:create	Grants permission to create a script.	write	script *	-
workspace:scripts:list	Grants permission to query the script list.	list	script *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:scripts:get	Grants permission to query script details.	read	script *	-
workspace:scripts:put	Grants permission to update a script.	write	script *	-
workspace:scripts:delete	Grants permission to delete a script.	write	script *	-
workspace:scripts:execute	Grants permission to run scripts or commands in batches.	write	script *	-
			desktop *	-
workspace:scripts:getRecordDetail	Grants permission to query script or command execution record details.	read	script *	-
workspace:scripts:listRecords	Grants permission to query script execution records.	list	script *	-
workspace:scripts:listTasks	Grants permission to query script tasks.	list	script *	-
workspace:scripts:retry	Grants permission to retry a script.	write	script *	-
workspace:scripts:stop	Grants permission to stop a script or command execution task.	write	script *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:scripts:download	Grants permission to download a script output record.	write	script *	-
workspace:tenants:getShareSpaceConfig	Grants permission to query collaboration configurations.	read	-	-
workspace:tenants:updateShareSpaceConfig	Grants permission to modify collaboration configurations.	write	-	-
workspace:authConfigs:getStatus	Grants permission to query the authentication status.	read	-	-
workspace:privacystatements:sign	Grants permission to sign the privacy statement.	write	-	-
workspace:sites:get	Grants permission to query site information.	read	-	-
workspace:sites:add	Grants permission to add a site.	write	-	workspace:AccessMode
workspace:sites:delete	Grants permission to delete a site.	write	-	-
workspace:sites:updateAccessMode	Grants permission to change the site access mode.	write	-	workspace:AccessMode

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:sites:updateSubnets	Grants permission to change the site service subnet.	write	-	-
workspace:tenants:checkEnterpriseIds	Grants permission to check whether the enterprise ID has been used.	write	-	-
workspace:tenants:updateEnterpriseId	Grants permission to change the enterprise ID.	write	-	-
workspace:bandwidth:create	Grants permission to enable the Workspace bandwidth.	write	-	-
workspace:bandwidth:list	Grants permission to query the Workspace bandwidth list.	list	-	-
workspace:bandwidth:update	Grants permission to modify the Workspace bandwidth.	write	-	-
workspace:bandwidth:delete	Grants permission to cancel the Workspace bandwidth.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:bandwidth:getControlConfig	Grants permission to query the control configuration of the Workspace bandwidth.	read	-	-
workspace:bandwidth:updateControlConfig	Grants permission to modify the control configuration of the Workspace bandwidth.	write	-	-
workspace:bandwidth:createChangeOrder	Grants permission to create a Workspace bandwidth change order.	write	-	-
workspace:desktops:batchCreateSnapshots	Grants permission to create desktop snapshots in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchDeleteSnapshots	Grants permission to delete desktop snapshots in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:batchRestoreSnapshots	Grants permission to restore desktop snapshots in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listSnapshots	Grants permission to query desktop snapshots.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:desktops:verifyDesktopName	Grants permission to verify the desktop name.	write	-	-
workspace:networks:getAvailableIp	Grants permission to query available IP addresses of a subnet by subnet ID.	read	-	-
workspace:desktops:getAdStatus	Grants permission to query the AD network status.	read	-	-
workspace:networks:checkIpIfExist	Grants permission to check whether the IP address exists.	write	-	-
workspace:images:checkIfExist	Grants permission to check whether the image exists.	write	-	-
workspace:wdh:listDesktops	Grants permission to query desktops of a Workspace host.	list	wdh *	-
			-	g:EnterpriseProjectId
workspace:wdh:update	Grants permission to update Workspace host information.	write	wdh *	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:bindingPolicies:getTemplate	Grants permission to download the template for terminal-desktop binding.	read	-	-
workspace:bindingPolicies:import	Grants permission to import terminal-desktop binding in batches.	write	-	-
workspace:statistics:getRunState	Grants permission to collect statistics on running statuses.	read	-	-
workspace:statistics:getLoginState	Grants permission to collect statistics on login statuses.	read	-	-
workspace:networks:getUsingSubnets	Grants permission to query subnets being used.	read	-	-
workspace:networks:listPorts	Grants permission to query ports.	list	-	-
workspace:renderDesktops:createConsole	Grants permission to obtain the URL for remote login to the console.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:renderDesktops:resize	Grants permission to change rendering desktop specifications.	write	-	-
workspace:exclusiveHosts:resizeLites	Grants permission to modify exclusive host specifications.	write	exclusiveHost *	g:EnterpriseProjectId
workspace:desktops:getMonitor	Grants permission to query desktop monitoring information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDetachInfo	Grants permission to query users unbound from the desktop.	list	desktop *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:desktops:getSysprepVersion	Grants permission to query Sysprep version information.	read	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:networks:createNat	Grants permission to enable the Internet access function of the NAT Gateway.	write	-	-
workspace:networks:listNats	Grants permission to query the Internet access function of the NAT Gateway.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:networks:listSubnets	Grants permission to query subnets.	list	-	-
workspace:networks:listVpcs	Grants permission to query VPCs.	list	-	-
workspace:policyGroups:createTemplate	Grants permission to create a policy template.	write	-	-
workspace:policyGroups:listTemplate	Grants permission to query policy templates.	list	-	-
workspace:policyGroups:updateTemplate	Grants permission to update a policy template.	write	-	-
workspace:networks:listSecurityGroups	Grants permission to query security groups.	list	-	-
workspace:availabilityZones:getSummary	Grants permission to query AZ summary.	read	-	-
workspace:availabilityZones:get	Grants permission to query AZ details.	read	-	-
workspace:users:importUser	Grants permission to import a user list.	write	user *	-
workspace:users:uploadTemplate	Grants permission to import a desktop user list.	write	user *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:accessPolicies:update	Grants permission to update a specified access policy.	write	-	-
workspace:desktops:verifySource	Grants permission to verify desktop sources.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:desktops:listDesktopNetworks	Grants permission to query desktop network information in batches.	list	desktop *	-
workspace:desktops:batchChangeNetwork	Grants permission to switch desktop networks in batches.	write	desktop *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:get	Grants permission to query task details.	read	-	-
workspace:accessPolicies:importIp	Grants permission to import the IP address list.	write	-	-
workspace:accessPolicies:getIpImportTemplate	Grants permission to download the template for importing IP addresses.	read	-	-
workspace:sites:listEdgeSites	Grants permission to query edge sites.	list	-	-
workspace:sites:checkEdgeSiteResources	Grants permission to verify edge site resources.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:ou:listAdOus	Grants permission to query OU information in the AD domain.	list	-	-
workspace:ou:listOuUsers	Grants permission to query user information in the OU.	list	-	-
workspace:ou:importUsersByOU	Grants permission to import OU users.	write	-	-
workspace:appGroup:list	Grants permission to query application groups.	list	appGroup *	-
workspace:appGroup:create	Grants permission to create an application group.	write	appGroup *	-
			serverGroup	-
workspace:appGroup:delete	Grants permission to delete an application group.	write	appGroup *	-
workspace:appGroup:get	Grants permission to query application group details.	read	appGroup *	-
workspace:appGroup:update	Grants permission to modify an application group.	write	appGroup *	-
			serverGroup	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:app:listPublishedApp	Grants permission to query published applications.	list	app *	-
			appGroup *	-
workspace:app:publish	Grants permission to publish an application.	write	app *	-
			appGroup *	-
workspace:app:get	Grants permission to query application details.	read	app *	-
			appGroup *	-
workspace:app:update	Grants permission to modify application information.	write	app *	-
			appGroup *	-
workspace:app:deleteIcon	Grants permission to delete a custom application icon.	write	app *	-
			appGroup *	-
workspace:app:uploadIcon	Grants permission to modify a custom application icon.	write	app *	-
			appGroup *	-
workspace:app:check	Grants permission to verify applications.	write	app *	-
			appGroup *	-
workspace:app:batchDisable	Grants permission to disable applications in batches.	write	app *	-
			appGroup *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:app:batchEnable	Grants permission to enable applications in batches.	write	app *	-
			appGroup *	-
workspace:app:unpublish	Grants permission to unpublish applications in batches.	write	app *	-
			appGroup *	-
workspace:appGroup:listPublishableApp	Grants permission to query applications that can be published.	list	appGroup *	-
workspace:appGroup:batchDeleteAuthorization	Grants permission to remove application group authorization.	write	appGroup *	-
			user	-
			userGroup	-
workspace:appGroup:disassociate	Grants permission to disassociate a service group from all application groups.	write	-	-
workspace:appGroup:listAuthorization	Grants permission to query application group authorization records.	list	appGroup *	-
workspace:appGroup:addAuthorization	Grants permission to add application group authorization.	write	appGroup *	-
			user	-
			userGroup	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appGroup:batchDelete	Grants permission to delete application groups in batches.	write	appGroup *	-
workspace:appGroup:check	Grants permission to verify an application group.	write	-	-
workspace:serverGroup:list	Grants permission to query server groups.	list	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:create	Grants permission to create a server group.	write	serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:serverGroup:delete	Grants permission to delete a server group.	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:get	Grants permission to query a specified server group.	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:update	Grants permission to modify a server group.	write	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:serverGroup:getServerState	Grants permission to query server statuses in a specified server group.	read	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:serverGroup:listDetail	Grants permission to query basic information about a tenant server group.	list	serverGroup *	-
workspace:serverGroup:getRestrict	Grants permission to query specified tenant server groups.	read	serverGroup *	-
workspace:serverGroup:validate	Grants permission to verify a server group.	write	serverGroup *	-
workspace:serverGroup:tagResource	Grants permission to add a tag to a server group.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:unTagResource	Grants permission to delete a tag from a server group.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:listTagsForResource	Grants permission to query server group tags.	list	serverGroup *	-
			-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:serverGroup:listTags	Grants permission to query tags on all servers of a tenant.	list	serverGroup *	-
workspace:serverGroup:batchCreateTags	Grants permission to add server group tags in batches.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:serverGroup:batchDeleteTags	Grants permission to delete server group tags in batches.	tagging	serverGroup *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			-	• g:RequestTag/<tag-key> • g:TagKeys
workspace:server:list	Grants permission to query servers.	list	server *	-
workspace:server:delete	Grants permission to delete a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:get	Grants permission to query a specified server.	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:update	Grants permission to modify a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:changeImage	Grants permission to modify a server image.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:server:reinstall	Grants permission to reinstall a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:getVncUrl	Grants permission to obtain a VNC login address.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:list	Grants permission to query the latest versions of all HDAs of a tenant.	list	-	-
workspace:accessAgent:batchUpgrade	Grants permission to upgrade the HDA version of servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:accessAgent:listLatestVersion	Grants permission to query the latest HDA version of a tenant.	list	-	-
workspace:server:listAccessAgentDetails	Grants permission to query HDA information of a server.	list	server *	-
workspace:accessAgent:getUpgradeFlag	Grants permission to query HDA upgrade notification flags.	read	-	-
workspace:accessAgent:updateUpgradeFlag	Grants permission to update an HDA upgrade notification flag.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:accessAgent:listUpgradeRecords	Grants permission to query HDA upgrade tracing records of a server.	list	-	-
workspace:server:batchDelete	Grants permission to delete servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchChangeMaintainMode	Grants permission to mark the server maintenance status.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReboot	Grants permission to restart a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchRejoinDomain	Grants permission to add servers to a domain again in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStart	Grants permission to start a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchStop	Grants permission to stop a server.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchUpdateTsvi	Grants permission to update virtual session IP configurations of servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:server:create	Grants permission to create an APS.	write	server *	-
			serverGroup *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys • g:EnterpriseProjectId
workspace:server:batchMigrateHosts	Grants permission to migrate servers at the source Workspace host to the destination one.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
			wdh *	-
workspace:server:getMetricData	Grants permission to query monitoring information of an APS.	read	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:jobs:batchDeleteSubJobs	Grants permission to delete subtasks in batches.	write	-	-
workspace:jobs:countSubJobs	Grants permission to query the number of subtasks.	list	-	-
workspace:appWarehouse:authorizeObs	Grants permission to obtain the AK/SK uploaded to an OBS bucket.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:appWarehouse:batchDeleteApp	Grants permission to delete specified applications from the application repository in batches.	write	-	-
workspace:appWarehouse:ListWarehouseApps	Grants permission to query applications in a tenant application repository.	list	-	-
workspace:appWarehouse:createApp	Grants permission to add an application to the application repository.	write	-	-
workspace:appWarehouse:deleteApp	Grants permission to delete a specified application from the application repository.	write	-	-
workspace:appWarehouse:uploadAppIcon	Grants permission to upload an icon file to the application repository.	write	-	-
workspace:appWarehouse:createBucketOrAcl	Grants permission to add a bucket or authorize access to a bucket.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:images:listImageJobs	Grants permission to query tasks of a tenant.	list	-	-
workspace:images:getImageJob	Grants permission to query task details.	read	-	-
workspace:imageServer:list	Grants permission to query image instances.	list	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:create	Grants permission to create an image instance.	write	imageServer *	-
			-	g:EnterpriseProjectId
workspace:imageServer:get	Grants permission to query a specified image instance.	read	imageServer *	g:EnterpriseProjectId
workspace:imageServer:update	Grants permission to modify an image instance.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:attachApp	Grants permission to distribute software information to image instances.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listLatestAttachedApp	Grants permission to query information about the latest distributed software.	list	imageServer *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:imageServer:recreate	Grants permission to build an Application Streaming image.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:batchDelete	Grants permission to delete image instances in batches.	write	imageServer *	g:EnterpriseProjectId
workspace:imageServer:listImageSubJobs	Grants permission to query subtasks.	list	-	-
workspace:imageServer:batchDeleteImageSubJobs	Grants permission to delete subtasks in batches.	write	-	-
workspace:imageServer:countImageSubJobs	Grants permission to query the number of subtasks.	read	-	-
workspace:appGroup:listMailRecord	Grants permission to query records of sending emails on application group authorization.	list	-	-
workspace:appGroup:resendMail	Grants permission to resend an email on application group authorization (based on authorization email records).	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:storage:listPersistentStorage	Grants permission to query Workspace storage space.	list	storage *	-
workspace:storage:createPersistentStorage	Grants permission to create Workspace storage space.	write	storage *	-
workspace:storage:deletePersistentStorage	Grants permission to delete Workspace storage space.	write	storage *	-
workspace:storage:updateUserFolderAssignment	Grants permission to create a personal storage directory.	write	storage *	-
workspace:storage:updateShareFolderAssignment	Grants permission to change members of a shared directory.	write	storage *	-
workspace:storage:createShareFolder	Grants permission to create a shared storage directory.	write	storage *	-
workspace:storage:deleteStorageClaim	Grants permission to delete a shared directory.	write	storage *	-
workspace:storage:deleteUserStorageAttachment	Grants permission to delete a personal storage directory.	write	storage *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:storage:batchDeletePersistentStorage	Grants permission to delete Workspace storage space in batches.	write	storage *	-
workspace:storage:listStorageAssignment	Grants permission to query personal storage directories.	list	storage *	-
workspace:storage:listShareFolder	Grants permission to query shared storage directories.	list	storage *	-
workspace:policyGroups:deleteTemplate	Grants permission to delete a policy template.	write	-	-
workspace:privacystatements:get	Grants permission to query the latest privacy statement.	read	-	-
workspace:scalingPolicy:delete	Grants permission to delete an auto scaling policy.	write	-	-
workspace:scalingPolicy:list	Grants permission to query auto scaling policies of a server group.	read	-	-
workspace:scalingPolicy:create	Grants permission to add or modify an auto scaling policy.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:session:listAppConnection	Grants permission to query application usage records.	write	-	-
workspace:session:logoffUserSession	Grants permission to log out of a session.	write	-	-
workspace:session:listUserConnection	Grants permission to query user login records.	write	-	-
workspace:session:listSessionByUserName	Grants permission to query current sessions by username.	list	-	-
workspace:storagePolicy:create	Grants permission to add or update a custom policy for storage directory access.	write	storage *	-
workspace:storagePolicy:list	Grants permission to query policies for storage directory access.	list	storage *	-
workspace:storage:listSfs3Storage	Grants permission to query SFS 3.0.	list	storage *	-
workspace:baseResource:list	Grants permission to query AZs.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:tenants:listConfigInfo	Grants permission to query enterprise system configurations.	list	-	-
workspace:tenants:active	Grants permission to activate and initialize a tenant service.	write	-	-
workspace:tenants:listTenantProfile	Grants permission to query tenant information.	list	-	-
workspace:server:listServerMetricData	Grants permission to query server monitoring data.	list	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:session:listSessions	Grants permission to query enterprise sessions.	list	-	-
workspace:appWarehouse:updateApp	Grants permission to update an application in the application repository.	write	-	-
workspace:server:batchChangeImage	Grants permission to switch server images in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId
workspace:server:batchReinstall	Grants permission to reinstall servers in batches.	write	server *	• g:ResourceTag/<tag-key> • g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
workspace:tenants:updateAccessAddressBackupConfig	Grants permission to modify the backup configuration of the Workspace access address.	write	-	-
workspace:tenants:listAccessAddressBackupConfig	Grants permission to obtain the backup configuration of the Workspace access address.	list	-	-
workspace:desktops:listWithConnectStatus	Grants permission to query desktop connection statuses.	list	-	-
workspace:orders:createDesktopOrder	Grants permission to create a desktop order.	write	-	-
workspace:products:listHourPackageProducts	Grants permission to query available hourly packages.	list	-	-

Each API of Workspace supports one or more actions. **Table 5-205** lists the supported actions and dependencies.

Table 5-205 Actions and dependencies supported by Workspace APIs

API	Action	Dependency
GET /v2/{project_id}/auth-config/method-config	workspace:authConfigs:get	-

API	Action	Dependency
PUT /v2/{project_id}/auth-config/method-config	workspace:authConfigs:update	-
GET /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:get	-
PUT /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:update	-
POST /v2/{project_id}/workspace-jobs/{job_id}/actions	workspace:jobs:retry	-
GET /v2/{project_id}/quotas	workspace:quotas:get	-
GET /v2/{project_id}/tenants/roles	workspace:tenants:getRoles	-
GET /v2/{project_id}/tenant-configs	workspace:tenants:ListConfig	-
PUT /v2/{project_id}/tenant-configs	workspace:tenants:updateConfig	-
GET /v2/{project_id}/nat-mapping-configs	workspace:natMappings:getConfig	-
PUT /v2/{project_id}/nat-mapping-configs	workspace:natMappings:updateConfig	-
GET /v2/{project_id}/workspaces	workspace:tenants:get	• vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get

API	Action	Dependency
POST /v2/{project_id}/workspaces	workspace:tenants:open	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	Action	Dependency
DELETE /v2/{project_id}/workspaces	workspace:tenants:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	Action	Dependency
PUT /v2/{project_id}/workspaces	workspace:tenants:update	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
GET /v2/{project_id}/workspaces/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/workspaces/lock-status	workspace:tenants:unlock	-

API	Action	Dependency
POST /v2/{project_id}/agencies	workspace:agencies:create	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:createServiceLinkedAgencyV5 • iam:roles:getRole • iam:roles:listRoles • iam:agencies:getAgency • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:listRolesForAgencyOnProject • iam:permissions:grantRoleToAgencyOnProject
GET /v2/{project_id}/agencies	workspace:agencies:get	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:getAgency • iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject
POST /v3/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:commitAiAccelerateJob	-
POST /v2/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:createAiAccelerateJob	-
GET /v2/{project_id}/ai-accelerate-job/{job_id}	workspace:desktops:getAiAccelerateJob	-
POST /v2/{project_id}/sysprep	workspace:desktops:getSysPrepInfo	-
POST /v2/{project_id}/verification/batch-change-image	workspace:desktops:checkBatchChangeImage	ims:images:list
GET /v2/{project_id}/desktop-name-policies	workspace:tenants:listDesktopNamePolicies	-
POST /v2/{project_id}/desktop-name-policies	workspace:tenants:createDesktopNamePolicy	-

API	Action	Dependency
PUT /v2/{project_id}/desktop-name-policies/{policy_id}	workspace:tenants:updateDesktopName-Policy	-
POST /v2/{project_id}/desktop-name-policies/batch-delete	workspace:tenants:batchDeleteDesktop-NamePolicies	-
POST /v2/{project_id}/desktop-pools	workspace:desktopPools:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktop-pools	workspace:desktopPools:list	ims:images:list
PUT /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:update	-
DELETE /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:delete	-
GET /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:get	ims:images:list

API	Action	Dependency
POST /v2/{project_id}/desktop-pools/{pool_id}/expand	workspace:desktopPools:expand	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
POST /v2/{project_id}/desktop-pools/{pool_id}/resize	workspace:desktopPools:resize	• vpc:subnets:get • ims:images:list
POST /v2/{project_id}/desktop-pools/{pool_id}/rebuild	workspace:desktopPools:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-add	workspace:desktopPools:batchAddVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-delete	workspace:desktopPools:batchDeleteVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-expand	workspace:desktopPools:batchExpandVolumes	-

API	Action	Dependency
POST /v2/{project_id}/desktop-pools/{pool_id}/action	workspace:desktopPools:operate	-
GET /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:listUsers	-
POST /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:authorizeUsers	ims:images:list
GET /v2/{project_id}/desktop-pools/{pool_id}/desktops	workspace:desktopPools:listDesktops	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-pools/script-execution-tasks/detail	workspace:desktopPools:listScriptTasks	-
POST /v2/{project_id}/desktop-pools/{pool_id}/script-executions	workspace:desktopPools:executeScripts	-
POST /v2/{project_id}/desktop-pools/{pool_id}/notifications	workspace:desktopPools:sendNotifications	-
GET /v3/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list

API	Action	Dependency
POST /v2/{project_id}/desktops	workspace:desktops:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • eip:publicIps:get • eip:publicIps:list • eip:publicIps:create • eip:publicIps:associateInstance • eip:publicIps:delete • eip:publicIps:createTags • vpc:quotas:list • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktops	workspace:desktops:list	-
PUT /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:update	-
DELETE /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/batch-delete	workspace:desktops:batchDelete	• vpc:ports:get • vpc:ports:delete

API	Action	Dependency
POST /v2/{project_id}/desktops/logoff	workspace:desktops:logoff	-
GET /v2/{project_id}/desktops/detail	workspace:desktops:listDetail	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/action	workspace:desktops:operate	-
POST /v2/{project_id}/desktops/resize	workspace:desktops:resize	• vpc:subnets:get • ims:images:list
GET /v2/{project_id}/connections/status	workspace:desktops:getConnectStatus	-
GET /v2/{project_id}/desktops/status	workspace:desktops:ListStatus	-
POST /v2/{project_id}/desktops/rebuild	workspace:desktops:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/actions	workspace:desktops:getActions	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-consoles	workspace:desktops:createConsole	-
PUT /v2/{project_id}/desktops/sids	workspace:desktops:updateSids	-
POST /v2/{project_id}/desktops/{desktop_id}/rejoin-domain	workspace:desktops:rejoinDomain	-

API	Action	Dependency
POST /v2/{project_id}/desktops/desktop-to-image	workspace:desktops:createImage	• ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
POST /v2/{project_id}/desktops/batch-detach	workspace:desktops:batchDetach	vpc:ports:get
POST /v2/{project_id}/desktops/detach	workspace:desktops:detach	vpc:ports:get
POST /v2/{project_id}/desktops/attach	workspace:desktops:attach	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:getNetwork	• vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list

API	Action	Dependency
PUT /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:changeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/exclusive-hosts/{host_id}/desktops	workspace:exclusiveHosts:listDesktops	-
GET /v2/{project_id}/all-desktops	workspace:desktops:listAll	-
GET /v2/{project_id}/desktop-associate/discover-vm/infos	workspace:desktopAssociate:listDiscoverVmInfo	-
POST /v2/{project_id}/desktop-associate/tasks	workspace:desktopAssociate:startTask	-
POST /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:switchScanTask	-
GET /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:getScanTaskSwitch	-
PUT /v2/{project_id}/desktops/maintenance-mode	workspace:desktops:setMaintenanceMode	-
POST /v2/{project_id}/desktops/pre-batch-attach	workspace:desktops:prepAttachUsers	-

API	Action	Dependency
POST /v2/{project_id}/desktops/batch-attach	workspace:desktops:batchAttachUsers	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
PUT /v2/{project_id}/desktops/change-username	workspace:desktops:changeUsername	-
POST /v2/{project_id}/desktops/notifications	workspace:desktops:sendNotifications	-
POST /v2/{project_id}/desktops/{desktop_id}/migrate	workspace:desktops:migrate	• vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:delete • vpc:ports:update • vpc:ports:get
GET /v2/{project_id}/desktops/agents	workspace:desktops:listAgents	-
POST /v2/{project_id}/desktops/agents	workspace:desktops:batchInstallAgents	-
GET /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:listTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/{desktop_id}/tags/{key}	workspace:desktops:untag	-
GET /v2/{project_id}/desktops/tags	workspace:desktops:listProjectTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags/action	workspace:desktops:operateTags	-

API	Action	Dependency
POST /v2/{project_id}/desktops/resource_instances/action	workspace:desktops:listByTags	-
POST /v2/{project_id}/desktops/batch-tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/batch-tags	workspace:desktops:untag	-
POST /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:create	• vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:subnets:get • vpc:vpcs:get
GET /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:list	-
POST /v2/{project_id}/exclusive-hosts/check-limits	workspace:exclusiveHosts:check	-
GET /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:get	• nat:snatRules:list • eip:publicIps:list
PUT /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:update	-
DELETE /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:delete	-
GET /v2/{project_id}/market-images	workspace:mkp:listImages	ims:images:list
GET /v2/{project_id}/mkp/commodities/commodity-ids	workspace:mkp:listCommodityInfos	-
POST /v2/{project_id}/mkp/order	workspace:mkp:createOrder	-

API	Action	Dependency
POST /v2/{project_id}/mkp/product-reserve	workspace:mkp:listListProductReserve	-
GET /v2/{project_id}/mkp/commodities	workspace:mkp:listCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/{commodity_id}/relation-commodities	workspace:mkp:listRelationCommodity-Details	-
GET /v2/{project_id}/mkp/commodities/agreements	workspace:mkp:listCommodityAgreements	-
GET /v2/{project_id}/eips	workspace:networks:listEips	• eip:publicIps:list • eip:bandwidths:list
POST /v2/{project_id}/eips	workspace:networks:createEips	• vpc:quotas:list • eip:publicIps:create • eip:publicIps:associateInstance
POST /v2/{project_id}/eips/binding	workspace:networks:bindEips	• eip:publicIps:associateInstance • eip:publicIps:get
POST /v2/{project_id}/eips/unbinding	workspace:networks:unbindEips	• eip:publicIps:list • eip:publicIps:disassociateInstance
GET /v2/{project_id}/eips/quotas	workspace:networks:getEipQuota	vpc:quotas:list
GET /v2/{project_id}/nat-gateways	workspace:networks:ListNatGateways	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/periodic/subscribe/order	workspace:orders:create	• ims:images:list • vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • bss:order:update

API	Action	Dependency
POST /v2/{project_id}/periodic/{desktop_id}/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/change/batch-order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/desktop-pool/periodic/inquiry/add-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/extend-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/resize	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/periodic/inquiry/add-resources	workspace:orders:batchInquiry	ims:images:list
GET /v2/{project_id}/checkOrderLimits	workspace:quotas:check	-
POST /v2/{project_id}/render-desktops	workspace:renderDesktops:create	• ims:images:list • ims:images:share • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get

API	Action	Dependency
DELETE /v2/{project_id}/render-desktops	workspace:renderDesktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/render-desktops	workspace:renderDesktops:list	-
POST /v2/{project_id}/render-desktops/action	workspace:renderDesktops:action	-
GET /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:getFuture	-
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
POST /v2/{project_id}/scheduled-tasks/{task_id}/records/export	workspace:scheduledTasks:exportRecords	-
POST /v2/{project_id}/user/share-resources	workspace:users:subscribeSharer	-
POST /v2/{project_id}/desktop/sub-resources	workspace:desktops:addSubResources	-

API	Action	Dependency
POST /v2/{project_id}/desktop/delete-sub-resources	workspace:desktops:deleteSubResources	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:createSnapshots	-
GET /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:getSnapshots	-
DELETE /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:deleteSnapshots	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots/restore	workspace:desktops:restoreBySnapshot	-
GET /v2/{project_id}/statistics	workspace:statistics:listDesktopStatus	-
GET /v2/{project_id}/desktops/statistics/unused	workspace:statistics:getUnused	-
POST /v2/{project_id}/desktops/statistics/used	workspace:statistics:getUsed	-
GET /v3/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:getConfig	-
POST /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:createConfig	-
GET /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:get	-
POST /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:add	-
PUT /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:update	-

API	Action	Dependency
POST /v2/{project_id}/terminals/binding-desktops/batch-delete	workspace:bindingPolicies:delete	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/batch-delete	workspace:volumes:delete	-
POST /v2/{project_id}/volumes	workspace:volumes:batchAdd	-
POST /v2/{project_id}/volumes/expand	workspace:volumes:batchExpand	-
GET /v2/{project_id}/hosts/types	workspace:wdh:getType	-
GET /v2/{project_id}/hosts	workspace:wdh:get	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:getRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:createRemoteAssistance	-
DELETE /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:cancelRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes	workspace:volumes:add	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/{volume_id}/expand	workspace:volumes:expand	-
GET /v2/{project_id}/dss-pools/detail	workspace:volumes:listDssPoolsDetail	dss:pools:list
GET /v2/{project_id}/common/timezones	workspace:common:listTimezones	-
GET /v3/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/images	workspace:images:list	ims:images:list

API	Action	Dependency
POST /v2/{project_id}/policy-groups/import	workspace:policyGroups:import	-
POST /v2/{project_id}/access-policy	workspace:accessPolicies:create	-
GET /v2/{project_id}/access-policy	workspace:accessPolicies:get	-
DELETE /v2/{project_id}/access-policy	workspace:accessPolicies:delete	-
GET /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:getTarget	-
PUT /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:updateTarget	-
GET /v2/{project_id}/products	workspace:products:listDesktopProducts	ecs:cloudServerFlavors:get
GET /v2/{project_id}/products/sharer	workspace:products:listSharerProducts	-
GET /v2/{project_id}/products/adninternet	workspace:products:listInternetProducts	-
GET /v2/{project_id}/availability-zones	workspace:availabilityZones:list	-
GET /v2/{project_id}/groups/export	workspace:userGroups:export	-
POST /v3/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/import	workspace:users:import	-
GET /v3/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
GET /v2/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
POST /v2/{project_id}/users/{user_id}/actions	workspace:users:operate	-

API	Action	Dependency
GET /v2/{project_id}/users/{user_id}/random-password	workspace:users:randomPassword	-
DELETE /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:deleteOtps	-
POST /v2/{project_id}/users/{user_id}/resend-email	workspace:users:resendEmail	-
GET /v2/{project_id}/connections/desktops	workspace:connections:securityList	-
GET /v2/{project_id}/connections/desktops/export	workspace:connections:securityExport	-
GET /v2/{project_id}/connections/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/desktops/connections	workspace:connections:securityList	-
GET /v2/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/desktops/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/groups	workspace:userGroups:list	-
POST /v2/{project_id}/groups	workspace:userGroups:create	-
POST /v2/{project_id}/groups/batch-delete	workspace:userGroups:batchDelete	-
DELETE /v2/{project_id}/groups/{group_id}	workspace:userGroups:delete	-
PUT /v2/{project_id}/groups/{group_id}	workspace:userGroups:update	-
POST /v2/{project_id}/groups/{group_id}/actions	workspace:userGroups:operate	-
GET /v2/{project_id}/groups/{group_id}/users	workspace:userGroups:getUsers	-

API	Action	Dependency
GET /v2/{project_id}/workspace-sub-jobs	workspace:jobs:listSubJobs	-
POST /v2/{project_id}/workspace-sub-jobs/batch-delete	workspace:jobs:deleteSubJobRecords	-
GET /v2/{project_id}/ous	workspace:ou:get	-
POST /v2/{project_id}/ous	workspace:ou:create	-
DELETE /v2/{project_id}/ous/{ou_id}	workspace:ou:delete	-
PUT /v2/{project_id}/ous/{ou_id}	workspace:ou:update	-
GET /v2/{project_id}/policy-groups	workspace:policyGroups:list	-
POST /v2/{project_id}/policy-groups	workspace:policyGroups:create	-
DELETE /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:delete	-
GET /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:update	-
POST /v2/{project_id}/policy-groups/export	workspace:policyGroups:export	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:updatePolicies	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:listTargets	-

API	Action	Dependency
PUT /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:updateTargets	-
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v2/{project_id}/policy-groups/original-policies	workspace:policyGroups:getOriginalPolicies	-
GET /v2/{project_id}/users	workspace:users:list	-
POST /v2/{project_id}/users	workspace:users:create	-
DELETE /v2/{project_id}/users/{user_id}	workspace:users:delete	-
GET /v2/{project_id}/users/{user_id}	workspace:users:get	-
PUT /v2/{project_id}/users/{user_id}	workspace:users:update	-
POST /v2/{project_id}/users/batch-delete	workspace:users:batchDelete	-
POST /v2/{project_id}/users/password	workspace:users:resetPassword	-
POST /v2/{project_id}/users/password-token	workspace:users:checkResetPasswordToken	-
GET /v2/{project_id}/users/desktop-users/template	workspace:users:getTemplate	-
POST /v2/{project_id}/users/exist	workspace:users:checkExist	-
GET /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:listOtps	-
GET /v2/{project_id}/users/template/download	workspace:users:getImportTemplate	-
POST /v2/{project_id}/users/export	workspace:users:export	-

API	Action	Dependency
POST /v2/{project_id}/users/batch-create	workspace:users:batchCreate	-
GET /v2/{project_id}/volume/products	workspace:products:listVolumeProducts	-
GET /v2/{project_id}/export-tasks	workspace:tenants:listExportTasks	-
POST /v2/{project_id}/export-tasks/batch-delete	workspace:tenants:deleteExportTasks	-
GET /v2/{project_id}/export-tasks/{task_id}/download	workspace:tenants:exportData	-
GET /v2/{project_id}/alarms	workspace:statistics:listAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/alarms	workspace:statistics:getAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/growth-rate	workspace:statistics:getGrowthRate	-
GET /v2/{project_id}/statistics/metrics	workspace:statistics:getMetric	-
GET /v2/{project_id}/statistics/metrics/trend	workspace:statistics:getMetricTrend	-
PUT /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:updateNotificationRules	smn:topic:get
DELETE /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:deleteNotificationRules	-
POST /v2/{project_id}/statistics/notify-rules	workspace:statistics:createNotifyRules	smn:topic:get
GET /v2/{project_id}/statistics/notify-rules	workspace:statistics:listNotificationRules	-
GET /v2/{project_id}/statistics/notification-records	workspace:statistics:listNotificationRecords	-
GET /v2/{project_id}/statistics/metrics/desktops	workspace:statistics:listDesktopMetrics	-

API	Action	Dependency
GET /v2/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/users	workspace:statistics:listUserMetrics	-
GET /v2/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
GET /v3/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v3/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
POST /v1/{project_id}/app-center/buckets/actions/create-credential	workspace:appcenter:createBucketCredential	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-center/buckets	workspace:appcenter:createAndAuthorizeBucket	• obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/app-center/apps	workspace:appcenter:listApps	-
POST /v1/{project_id}/app-center/apps	workspace:appcenter:createApp	-
PATCH /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:updateApp	-
DELETE /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:deleteApp	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/auto-install	workspace:appcenter:installApp	-
GET /v1/{project_id}/app-center/apps/{app_id}/authorizations	workspace:appcenter:listAppAuthorizations	-

API	Action	Dependency
POST /v1/{project_id}/app-center/apps/{app_id}/actions/assign-authorizations	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-delete	workspace:appcenter:batchDeleteApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-disable	workspace:appcenter:batchDisableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-enable	workspace:appcenter:batchEnableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-assign-authorization	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-auto-install	workspace:appcenter:batchInstallApps	-
GET /v1/{project_id}/app-center/app-catalogs	workspace:appcenter:listAppCatalogs	-
GET /v1/{project_id}/app-center/jobs	workspace:appcenter:listJobs	-
POST /v1/{project_id}/app-center/jobs/actions/batch-delete	workspace:appcenter:batchDeleteJobs	-
POST /v1/{project_id}/app-center/jobs/actions/retry	workspace:appcenter:retryJobs	-
POST /v1/{project_id}/app-center/app-rules	workspace:appcenter:createAppRule	-
GET /v1/{project_id}/app-center/app-rules	workspace:appcenter:listAppRule	-
PATCH /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:updateAppRule	-

API	Action	Dependency
DELETE /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:deleteAppRule	-
POST /v1/{project_id}/app-center/app-rules/batch-delete	workspace:appcenter:batchDeleteAppRules	-
POST /v1/{project_id}/app-center/app-rules/actions/enable-rule-restriction	workspace:appcenter:enableRuleRestriction	-
POST /v1/{project_id}/app-center/app-rules/actions/disable-rule-restriction	workspace:appcenter:disableRuleRestriction	-
POST /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:addRestrictedRule	-
GET /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:listRestrictedRule	-
POST /v1/{project_id}/app-center/app-restricted-rules/actions/batch-delete	workspace:appcenter:deleteRestrictedRule	-
PATCH /v1/{project_id}/app-center/profiles	workspace:appcenter:updateTenantProfile	-
GET /v1/{project_id}/app-center/profiles	workspace:appcenter:listTenantProfiles	-
POST /v2/{project_id}/scripts	workspace:scripts:create	-
GET /v2/{project_id}/scripts	workspace:scripts:list	-
GET /v2/{project_id}/scripts/{script_id}	workspace:scripts:get	-
PUT /v2/{project_id}/scripts/{script_id}	workspace:scripts:put	-
DELETE /v2/{project_id}/scripts/{script_id}	workspace:scripts:delete	-
POST /v2/{project_id}/script-executions	workspace:scripts:execute	-

API	Action	Dependency
GET /v2/{project_id}/script-execution-records/{record_id}	workspace:scripts:getRecordDetail	-
GET /v2/{project_id}/script-execution-records	workspace:scripts:listRecords	-
GET /v2/{project_id}/script-execution-tasks	workspace:scripts:listTasks	-
POST /v2/{project_id}/script-executions/retry	workspace:scripts:retry	-
POST /v2/{project_id}/script-executions/stop	workspace:scripts:stop	-
POST /v2/{project_id}/script-execution-records/{record_id}/download	workspace:scripts:download	-
GET /v2/{project_id}/share-space/configuration	workspace:tenants:getShareSpaceConfig	-
PUT /v2/{project_id}/share-space/configuration	workspace:tenants:updateShareSpace-Config	-
GET /v2/{project_id}/auth-config/status	workspace:authConfigs:getStatus	-
POST /v2/{project_id}/privacystatement	workspace:privacystatements:sign	-
GET /v2/{project_id}/quotas/detail	workspace:quotas:get	-
GET /v2/{project_id}/sites	workspace:sites:get	-

API	Action	Dependency
POST /v2/{project_id}/sites	workspace:sites:add	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	Action	Dependency
DELETE /v2/{project_id}/sites/{site_id}	workspace:sites:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	Action	Dependency
PUT /v2/{project_id}/sites/{site_id}/access-mode	workspace:sites:updateAccessMode	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
PUT /v2/{project_id}/sites/{site_id}/subnet-ids	workspace:sites:updateSubnets	• vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get
GET /v2/{project_id}/tenants/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/tenants/lock-status	workspace:tenants:unlock	-

API	Action	Dependency
POST /v2/{project_id}/workspaces/enterprise-ids/check	workspace:tenants:checkEnterpriseIds	-
PUT /v2/{project_id}/workspaces/enterprise-id	workspace:tenants:updateEnterpriseId	-
POST /v2/{project_id}/bandwidths	workspace:bandwidth:create	-
GET /v2/{project_id}/bandwidths	workspace:bandwidth:list	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/update	workspace:bandwidth:update	-
DELETE /v2/{project_id}/bandwidths/{bandwidth_id}	workspace:bandwidth:delete	-
GET /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:getControlConfig	-
PUT /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:updateControlConfig	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/periodic/change/order	workspace:bandwidth:createChangeOrder	-
POST /v2/{project_id}/adns	workspace:bandwidth:create	-
GET /v2/{project_id}/adns	workspace:bandwidth:list	-
POST /v2/{project_id}/desktops-adn/batch-delete	workspace:bandwidth:delete	-
POST /v2/{project_id}/snapshots/batch-create	workspace:desktops:batchCreateSnapshots	-

API	Action	Dependency
POST /v2/{project_id}/snapshots/batch-delete	workspace:desktops:batchDeleteSnapshots	-
POST /v2/{project_id}/snapshots/batch-restore	workspace:desktops:batchRestoreSnapshots	-
GET /v2/{project_id}/snapshots	workspace:desktops:listSnapshots	-
POST /v2/{project_id}/verification/desktop-name	workspace:desktops:verifyDesktopName	-
GET /v2/{project_id}/subnets/{subnet_id}/available-ip	workspace:networks:getAvailableIp	-
GET /v2/{project_id}/ad/status	workspace:desktops:getAdStatus	-
GET /v2/{project_id}/ip-exist	workspace:networks:checkIpIfExist	-
POST /v2/{project_id}/desktops/check-images	workspace:images:checkIfExist	ims:images:list
GET /v2/{project_id}/hosts/{host_id}/servers	workspace:wdh:listDesktops	-
PUT /v2/{project_id}/hosts	workspace:wdh:update	-
GET /v2/{project_id}/terminals/binding-desktops/template	workspace:bindingPolicies:getTemplate	-
POST /v2/{project_id}/terminals/binding-desktops/template/import	workspace:bindingPolicies:import	-
GET /v2/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/desktops/statistics/run-state	workspace:statistics:getRunState	-
GET /v2/{project_id}/desktops/statistics/login-state	workspace:statistics:getLoginState	-

API	Action	Dependency
GET /v2/{project_id}/subnets/using-subnets	workspace:networks:getUsingSubnets	-
GET /v2/{project_id}/ports	workspace:networks:listPorts	-
GET /v2/{project_id}/render-desktops/{desktop_id}/remote-consoles	workspace:renderDesktops:createConsole	-
PUT /v2/{project_id}/render-desktops/resize	workspace:renderDesktops:resize	-
POST /v2/{project_id}/exclusive-hosts/{host_id}/resize-lites	workspace:exclusiveHosts:resizeLites	-
GET /services/v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-monitor/{desktop_id}	workspace:desktops:getMonitor	ces:metricData:get
GET /v2/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktops/{desktop_id}/detach-info	workspace:desktops:listDetachInfo	-
GET /v2/{project_id}/desktops/{desktop_id}/sysprep	workspace:desktops:getSysprepVersion	-

API	Action	Dependency
POST /v2/{project_id}/internet	workspace:networks:createNat	• vpc:ports:delete • vpc:ports:get • vpc:networks:get • eip:publicIps:create • eip:publicIps:update • eip:publicIps:delete • nat:snatRules:list • nat:snatRules:create • nat:natGateways:list • nat:natGateways:create
GET /v2/{project_id}/internet	workspace:networks:listNats	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/quotas/check	workspace:quotas:check	-
GET /v2/{project_id}/subnets	workspace:networks:listSubnets	• vpc:subnets:list • vpc:subnets:get
GET /v2/{project_id}/vpcs	workspace:networks:listVpcs	vpc:vpcs:list
POST /v2/{project_id}/policy-groups/policy-template	workspace:policyGroups:createTemplate	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
PUT /v2/{project_id}/policy-groups/policy-template/{policy_group_id}	workspace:policyGroups:updateTemplate	-
GET /v2/{project_id}/security-groups	workspace:networks:listSecurityGroups	-
GET /v2/{project_id}/availability-zones/summary	workspace:availabilityZones:getSummary	-
GET /v2/{project_id}/availability-zones/detail	workspace:availabilityZones:get	-
POST /v2/{project_id}/users/desktop-users/action/import	workspace:users:importUser	-

API	Action	Dependency
POST /v2/{project_id}/users/template-upload	workspace:users:uploadTemplate	-
PUT /v2/{project_id}/access-policy/{access_policy_id}	workspace:accessPolicies:update	-
POST /v2/{project_id}/desktops/{desktop_id}/verify-source	workspace:desktops:verifySource	-
GET /v2/{project_id}/desktops/networks	workspace:desktops:listDesktopNetworks	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
POST /v2/{project_id}/desktops/networks/batch-change	workspace:desktops:batchChangeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/workspace-jobs/{job_id}	workspace:jobs:get	-
POST /v2/{project_id}/ip/import	workspace:accessPolicies:importIp	-
GET /v2/{project_id}/ip/template/download	workspace:accessPolicies:getIpImportTemplate	-
GET /v2/{project_id}/wks-edge-sites	workspace:sites:listEdgeSites	• ies:edgeSite:list • ies:edgeSite:getMetricData
POST /v2/{project_id}/check-edge-site-resources	workspace:sites:checkEdgeSiteResources	• ies:edgeSite:list • ies:edgeSite:getMetricData

API	Action	Dependency
GET /v2/{project_id}/ad-ous	workspace:ou:listAdOus	-
GET /v2/{project_id}/ou-users	workspace:ou:listOuUsers	-
POST /v2/{project_id}/ou-users/import	workspace:ou:importUsersByOU	-
GET /v1/{project_id}/app-groups	workspace:appGroup:list	-
POST /v1/{project_id}/app-groups	workspace:appGroup:create	-
DELETE /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:delete	-
GET /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:update	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:listPublishedApp	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:publish	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:update	-
DELETE /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:deleteIcon	-

API	Action	Dependency
POST /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:uploadIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/check	workspace:app:check	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/disable	workspace:app:batchDisable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/enable	workspace:app:batchEnable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/batch-unpublish	workspace:app:unpublish	-
GET /v1/{project_id}/app-groups/{app_group_id}/publishable-app	workspace:appGroup:listPublishableApp	-
POST /v1/{project_id}/app-groups/actions/batch-delete-authorization	workspace:appGroup:batchDeleteAuthorization	-
POST /v1/{project_id}/app-groups/actions/disassociate-app-group	workspace:appGroup:disassociate	-
GET /v1/{project_id}/app-groups/actions/list-authorizations	workspace:appGroup:listAuthorization	-
POST /v1/{project_id}/app-groups/authorizations	workspace:appGroup:addAuthorization	-
POST /v1/{project_id}/app-groups/batch-delete	workspace:appGroup:batchDelete	-
POST /v1/{project_id}/app-groups/rules/validate	workspace:appGroup:check	-

API	Action	Dependency
GET /v1/{project_id}/app-server-groups	workspace:serverGroup:list	-
POST /v1/{project_id}/app-server-groups	workspace:serverGroup:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
DELETE /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:delete	-
GET /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:get	-
PATCH /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:update	ims:images:list
GET /v1/{project_id}/app-server-groups/{server_group_id}/state	workspace:serverGroup:getServerState	-
GET /v1/{project_id}/app-server-groups/actions/list	workspace:serverGroup:listDetail	-
GET /v1/{project_id}/app-server-groups/resources/restrict	workspace:serverGroup:getRestrict	-
POST /v1/{project_id}/app-server-groups/rules/validate	workspace:serverGroup:validate	-
POST /v1/{project_id}/server-group/{server_group_id}/tags/create	workspace:serverGroup:tagResource	-
DELETE /v1/{project_id}/server-group/{server_group_id}/tags/delete	workspace:serverGroup:unTagResource	-
GET /v1/{project_id}/server-group/{server_group_id}/tags	workspace:serverGroup:listTagsForResource	-
GET /v1/{project_id}/server-group/tags	workspace:serverGroup:listTags	-

API	Action	Dependency
POST /v1/{project_id}/server-group/tags/batch-create	workspace:serverGroup:batchCreateTags	-
DELETE /v1/{project_id}/server-group/tags/batch-delete	workspace:serverGroup:batchDeleteTags	-
GET /v1/{project_id}/app-servers	workspace:server:list	-
DELETE /v1/{project_id}/app-servers/{server_id}	workspace:server:delete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
GET /v1/{project_id}/app-servers/{server_id}	workspace:server:get	-
PATCH /v1/{project_id}/app-servers/{server_id}	workspace:server:update	-
POST /v1/{project_id}/app-servers/{server_id}/actions/change-image	workspace:server:changeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/{server_id}/actions/reinstall	workspace:server:reinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/app-servers/{server_id}/actions/vnc	workspace:server:getVncUrl	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:list	-
PATCH /v1/{project_id}/app-servers/access-agent/actions/upgrade	workspace:accessAgent:batchUpgrade	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:listLatestVersion	-
GET /v1/{project_id}/app-servers/access-agent/list	workspace:server:listAccessAgentDetails	-

API	Action	Dependency
GET /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:getUpgradeFlag	-
PATCH /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:updateUpgradeFlag	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:listUpgradeRecords	-
POST /v1/{project_id}/app-servers/actions/batch-delete	workspace:server:batchDelete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
PATCH /v1/{project_id}/app-servers/actions/batch-maint	workspace:server:batchChangeMaintainMode	-
PATCH /v1/{project_id}/app-servers/actions/batch-reboot	workspace:server:batchReboot	-
PATCH /v1/{project_id}/app-servers/actions/batch-rejoin-domain	workspace:server:batchRejoinDomain	-
PATCH /v1/{project_id}/app-servers/actions/batch-start	workspace:server:batchStart	-
PATCH /v1/{project_id}/app-servers/actions/batch-stop	workspace:server:batchStop	-
PATCH /v1/{project_id}/app-servers/actions/batch-update-tsvi	workspace:server:batchUpdateTsvi	• vpc:subnets:get • vpc:ports:update

API	Action	Dependency
POST /v1/{project_id}/app-servers/actions/create	workspace:server:create	• ims:images:list • ims:images:updateMemberStatus • ims:images:share • ims:images:get • vpc:securityGroups:get • vpc:securityGroupRules:get • vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:get • vpc:ports:delete • vpc:vpcs:get • dss:pools:list
PATCH /v1/{project_id}/app-servers/hosts/batch-migrate	workspace:server:batchMigrateHosts	-
GET /v1/{project_id}/app-servers/metric-data/{server_id}	workspace:server:getMetricData	-
GET /v1/{project_id}/app-server-sub-jobs	workspace:jobs:listSubJobs	-
POST /v1/{project_id}/app-server-sub-jobs/actions/batch-delete	workspace:jobs:batchDeleteSubJobs	-
GET /v1/{project_id}/app-server-sub-jobs/actions/count	workspace:jobs:countSubJobs	-
POST /v1/{project_id}/app-warehouse/action/authorize	workspace:appWarehouse:authorizeObs	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/actions/batch-delete	workspace:appWarehouse:batchDeleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
GET /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:ListWarehouseApps	-
POST /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:createApp	-

API	Action	Dependency
DELETE /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:deleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/apps/icon	workspace:appWarehouse:uploadAppIcon	obs:object:PutObject
POST /v1/{project_id}/app-warehouse/bucket-and-acl/create	workspace:appWarehouse:createBucketOrAcl	• obs:bucket:GetBucketAcl • obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/check/quota	workspace:quotas:get	-
GET /v1/{project_id}/image-server-jobs	workspace:images:listImageJobs	-
GET /v1/{project_id}/image-server-jobs/{job_id}	workspace:images:getImageJob	-
GET /v1/{project_id}/image-servers	workspace:imageServer:list	-
POST /v1/{project_id}/image-servers	workspace:imageServer:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:get	-
PATCH /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:update	-
POST /v1/{project_id}/image-servers/{server_id}/actions/attach-app	workspace:imageServer:attachApp	-
GET /v1/{project_id}/image-servers/{server_id}/actions/latest-attached-app	workspace:imageServer:listLatestAttachedApp	-

API	Action	Dependency
POST /v1/{project_id}/image-servers/{server_id}/actions/recreate-image	workspace:imageServer:recreate	• vpc:ports:get • vpc:subnets:get • ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
PATCH /v1/{project_id}/image-servers/actions/batch-delete	workspace:imageServer:batchDelete	-
GET /v1/{project_id}/image-server-sub-jobs	workspace:imageServer:listImageSubJobs	-
PATCH /v1/{project_id}/image-server-sub-jobs/actions/batch-delete	workspace:imageServer:batchDeleteImageSubJobs	-
GET /v1/{project_id}/image-server-sub-jobs/actions/count	workspace:imageServer:countImageSubJobs	-
GET /v2/{project_id}/job/{job_id}	workspace:jobs:get	-
GET /v1/{project_id}/mails	workspace:appGroup:listMailRecord	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
POST /v1/{project_id}/mails/actions/send-by-authorization	workspace:appGroup:resendMail	-
GET /v1/{project_id}/persistent-storages	workspace:storage:listPersistentStorage	-
POST /v1/{project_id}/persistent-storages	workspace:storage:createPersistentStorage	• obs:bucket:HeadBucket • obs:bucket:PutBucketPolicy • obs:bucket:PutBucketAcl • obs:bucket:PutBucketCORS

API	Action	Dependency
DELETE /v1/{project_id}/persistent-storages/{storage_id}	workspace:storage:deletePersistentStorage	• obs:object:GetObject • obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-folder	workspace:storage:updateUserFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-share-folder	workspace:storage:updateShareFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/create-share-folder	workspace:storage:createShareFolder	• obs:object:GetObject • obs:object:PutObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-storage-claim	workspace:storage:deleteStorageClaim	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-user-attachment	workspace:storage:deleteUserStorageAttachment	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/actions/batch-delete	workspace:storage:batchDeletePersistentStorage	-
GET /v1/{project_id}/persistent-storages/actions/list-attachments	workspace:storage:listStorageAssignment	-
GET /v1/{project_id}/persistent-storages/actions/list-share-folders	workspace:storage:listShareFolder	-
GET /v1/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/policy	workspace:policyGroups:listPolicies	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/target	workspace:policyGroups:listTargets	-

API	Action	Dependency
GET /v1/{project_id}/policy-groups/show/detail	workspace:policyGroups:listDetail	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
DELETE /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:deleteTemplate	-
PATCH /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:updateTemplate	-
GET /v1/{project_id}/privacy-statement	workspace:privacystatements:get	-
DELETE /v1/{project_id}/scaling-policy	workspace:scalingPolicy:delete	-
GET /v1/{project_id}/scaling-policy	workspace:scalingPolicy:list	-
PUT /v1/{project_id}/scaling-policy	workspace:scalingPolicy:create	-
GET /v1/{project_id}/schedule-task/{task_id}/execute-history	workspace:scheduledTasks:list	-
POST /v1/{project_id}/schedule-task	workspace:scheduledTasks:create	-
GET /v1/{project_id}/schedule-task/{execute_history_id}/execute-detail	workspace:scheduledTasks:getRecord	-
DELETE /v1/{project_id}/schedule-task/{task_id}	workspace:scheduledTasks:delete	-
POST /v1/{project_id}/schedule-task/future-executions	workspace:scheduledTasks:get	-
PATCH /v1/{project_id}/schedule-task/{task_id}	workspace:scheduledTasks:update	-
GET /v1/{project_id}/schedule-task/{task_id}/execute-history	workspace:scheduledTasks:listRecords	-

API	Action	Dependency
POST /v1/{project_id}/schedule-task/actions/batch-delete	workspace:scheduledTasks:batchDelete	-
POST /v1/{project_id}/session/app-connection	workspace:session:listAppConnection	-
POST /v1/{project_id}/session/logoff	workspace:session:logoffUserSession	-
POST /v1/{project_id}/session/user-connection	workspace:session:listUserConnection	-
GET /v1/{project_id}/session/user-session-info	workspace:session:listSessionByUserName	-
PUT /v1/{project_id}/storages-policy/actions/create-statements	workspace:storagePolicy:create	-
GET /v1/{project_id}/storages-policy/actions/list-statements	workspace:storagePolicy:list	-
GET /v1/{project_id}/users	workspace:users:list	-
GET /v1/persistent-storages/actions/list-sfs-storages	workspace:storage:listSfs3Storage	• obs:bucket:ListBucket • obs:bucket:GetBucketStorage • obs:bucket:ListAllMyBuckets
GET /v1/{project_id}/product	workspace:baseResource:list	ecs:availabilityZones:list
POST /v1/{project_id}/bundles/batch-query-config-info	workspace:tenants:listConfigInfo	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
POST /v1/{project_id}/tenant/action/active	workspace:tenants:active	-
GET /v1/{project_id}/tenant/profile	workspace:tenants:listTenantProfile	-

API	Action	Dependency
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
GET /v1/{project_id}/app-servers/server-metric-data/{server_id}	workspace:server:listServerMetricData	-
GET /v1/{project_id}/session/list-sessions	workspace:session:listSessions	-
PATCH /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:updateApp	-
POST /v1/{project_id}/app-servers/actions/batch-change-image	workspace:server:batchChangeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/actions/batch-reinstall	workspace:server:batchReinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v2/{project_id}/auth-config/method-config	workspace:authConfigs:get	-
PUT /v2/{project_id}/auth-config/method-config	workspace:authConfigs:update	-
GET /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:get	-
PUT /v2/{project_id}/assist-auth-config/method-config	workspace:assistAuthConfigs:update	-
POST /v2/{project_id}/workspace-jobs/{job_id}/actions	workspace:jobs:retry	-
GET /v2/{project_id}/quotas	workspace:quotas:get	-
GET /v2/{project_id}/tenants/roles	workspace:tenants:getRoles	-
GET /v2/{project_id}/tenant-configs	workspace:tenants:ListConfig	-
PUT /v2/{project_id}/tenant-configs	workspace:tenants:updateConfig	-

API	Action	Dependency
GET /v2/{project_id}/nat-mapping-configs	workspace:natMappings:getConfig	-
PUT /v2/{project_id}/nat-mapping-configs	workspace:natMappings:updateConfig	-
GET /v2/{project_id}/workspaces	workspace:tenants:get	• vpc:vpcs:get • vpc:subnets:get • vpc:securityGroups:get
POST /v2/{project_id}/workspaces	workspace:tenants:open	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	Action	Dependency
DELETE /v2/{project_id}/workspaces	workspace:tenants:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	Action	Dependency
PUT /v2/{project_id}/workspaces	workspace:tenants:update	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
GET /v2/{project_id}/workspaces/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/workspaces/lock-status	workspace:tenants:unlock	-

API	Action	Dependency
POST /v2/{project_id}/agencies	workspace:agencies:create	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:createServiceLinkedAgencyV5 • iam:roles:getRole • iam:roles:listRoles • iam:agencies:getAgency • iam:agencies:listAgencies • iam:agencies:createAgency • iam:permissions:listRolesForAgencyOnProject • iam:permissions:grantRoleToAgencyOnProject
GET /v2/{project_id}/agencies	workspace:agencies:get	• iam:agencies:listV5 • iam:agencies:getV5 • iam:agencies:getAgency • iam:agencies:listAgencies • iam:permissions:listRolesForAgencyOnProject
POST /v3/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:commitAiAccelerateJob	-
POST /v2/{project_id}/desktops/{desktop_id}/ai-accelerate-job	workspace:desktops:createAiAccelerateJob	-
GET /v2/{project_id}/ai-accelerate-job/{job_id}	workspace:desktops:getAiAccelerateJob	-
POST /v2/{project_id}/sysprep	workspace:desktops:getSysPrepInfo	-
POST /v2/{project_id}/verification/batch-change-image	workspace:desktops:checkBatchChangeImage	ims:images:list
GET /v2/{project_id}/desktop-name-policies	workspace:tenants:listDesktopNamePolicies	-
POST /v2/{project_id}/desktop-name-policies	workspace:tenants:createDesktopNamePolicy	-

API	Action	Dependency
PUT /v2/{project_id}/desktop-name-policies/{policy_id}	workspace:tenants:updateDesktopName-Policy	-
POST /v2/{project_id}/desktop-name-policies/batch-delete	workspace:tenants:batchDeleteDesktop-NamePolicies	-
POST /v2/{project_id}/desktop-pools	workspace:desktopPools:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktop-pools	workspace:desktopPools:list	ims:images:list
PUT /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:update	-
DELETE /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:delete	-
GET /v2/{project_id}/desktop-pools/{pool_id}	workspace:desktopPools:get	ims:images:list

API	Action	Dependency
POST /v2/{project_id}/desktop-pools/{pool_id}/expand	workspace:desktopPools:expand	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
POST /v2/{project_id}/desktop-pools/{pool_id}/resize	workspace:desktopPools:resize	• vpc:subnets:get • ims:images:list
POST /v2/{project_id}/desktop-pools/{pool_id}/rebuild	workspace:desktopPools:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-add	workspace:desktopPools:batchAddVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-delete	workspace:desktopPools:batchDeleteVolumes	-
POST /v2/{project_id}/desktop-pools/{pool_id}/volumes/batch-expand	workspace:desktopPools:batchExpandVolumes	-

API	Action	Dependency
POST /v2/{project_id}/desktop-pools/{pool_id}/action	workspace:desktopPools:operate	-
GET /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:listUsers	-
POST /v2/{project_id}/desktop-pools/{pool_id}/users	workspace:desktopPools:authorizeUsers	ims:images:list
GET /v2/{project_id}/desktop-pools/{pool_id}/desktops	workspace:desktopPools:listDesktops	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-pools/script-execution-tasks/detail	workspace:desktopPools:listScriptTasks	-
POST /v2/{project_id}/desktop-pools/{pool_id}/script-executions	workspace:desktopPools:executeScripts	-
POST /v2/{project_id}/desktop-pools/{pool_id}/notifications	workspace:desktopPools:sendNotifications	-
GET /v3/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list

API	Action	Dependency
POST /v2/{project_id}/desktops	workspace:desktops:create	• ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • eip:publicIps:get • eip:publicIps:list • eip:publicIps:create • eip:publicIps:associateInstance • eip:publicIps:delete • eip:publicIps:createTags • vpc:quotas:list • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get • dss:pools:list
GET /v2/{project_id}/desktops	workspace:desktops:list	-
PUT /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:update	-
DELETE /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/batch-delete	workspace:desktops:batchDelete	• vpc:ports:get • vpc:ports:delete

API	Action	Dependency
POST /v2/{project_id}/desktops/logoff	workspace:desktops:logoff	-
GET /v2/{project_id}/desktops/detail	workspace:desktops:listDetail	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
POST /v2/{project_id}/desktops/action	workspace:desktops:operate	-
POST /v2/{project_id}/desktops/resize	workspace:desktops:resize	• vpc:subnets:get • ims:images:list
GET /v2/{project_id}/connections/status	workspace:desktops:getConnectStatus	-
GET /v2/{project_id}/desktops/status	workspace:desktops:ListStatus	-
POST /v2/{project_id}/desktops/rebuild	workspace:desktops:rebuild	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/actions	workspace:desktops:getActions	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-consoles	workspace:desktops:createConsole	-
PUT /v2/{project_id}/desktops/sids	workspace:desktops:updateSids	-
POST /v2/{project_id}/desktops/{desktop_id}/rejoin-domain	workspace:desktops:rejoinDomain	-

API	Action	Dependency
POST /v2/{project_id}/desktops/desktop-to-image	workspace:desktops:createImage	• ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
POST /v2/{project_id}/desktops/batch-detach	workspace:desktops:batchDetach	vpc:ports:get
POST /v2/{project_id}/desktops/detach	workspace:desktops:detach	vpc:ports:get
POST /v2/{project_id}/desktops/attach	workspace:desktops:attach	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
GET /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:getNetwork	• vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list

API	Action	Dependency
PUT /v2/{project_id}/desktops/{desktop_id}/networks	workspace:desktops:changeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/exclusive-hosts/{host_id}/desktops	workspace:exclusiveHosts:listDesktops	-
GET /v2/{project_id}/all-desktops	workspace:desktops:listAll	-
GET /v2/{project_id}/desktop-associate/discover-vm/infos	workspace:desktopAssociate:listDiscoverVmInfo	-
POST /v2/{project_id}/desktop-associate/tasks	workspace:desktopAssociate:startTask	-
POST /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:switchScanTask	-
GET /v2/{project_id}/desktop-associate/discover-vm/switch	workspace:desktopAssociate:getScanTaskSwitch	-
PUT /v2/{project_id}/desktops/maintenance-mode	workspace:desktops:setMaintenanceMode	-
POST /v2/{project_id}/desktops/pre-batch-attach	workspace:desktops:prepAttachUsers	-

API	Action	Dependency
POST /v2/{project_id}/desktops/batch-attach	workspace:desktops:batchAttachUsers	• vpc:ports:get • ims:images:get • ims:images:list • ims:images:share • ims:images:updateMemberStatus • ims:images:deleteMember • ims:images:addMember
PUT /v2/{project_id}/desktops/change-username	workspace:desktops:changeUsername	-
POST /v2/{project_id}/desktops/notifications	workspace:desktops:sendNotifications	-
POST /v2/{project_id}/desktops/{desktop_id}/migrate	workspace:desktops:migrate	• vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:delete • vpc:ports:update • vpc:ports:get
GET /v2/{project_id}/desktops/agents	workspace:desktops:listAgents	-
POST /v2/{project_id}/desktops/agents	workspace:desktops:batchInstallAgents	-
GET /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:listTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/{desktop_id}/tags/{key}	workspace:desktops:untag	-
GET /v2/{project_id}/desktops/tags	workspace:desktops:listProjectTags	-
POST /v2/{project_id}/desktops/{desktop_id}/tags/action	workspace:desktops:operateTags	-

API	Action	Dependency
POST /v2/{project_id}/desktops/resource_instances/action	workspace:desktops:listByTags	-
POST /v2/{project_id}/desktops/batch-tags	workspace:desktops:tag	-
DELETE /v2/{project_id}/desktops/batch-tags	workspace:desktops:untag	-
POST /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:create	• vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:subnets:get • vpc:vpcs:get
GET /v2/{project_id}/exclusive-hosts	workspace:exclusiveHosts:list	-
POST /v2/{project_id}/exclusive-hosts/check-limits	workspace:exclusiveHosts:check	-
GET /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:get	• nat:snatRules:list • eip:publicIps:list
PUT /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:update	-
DELETE /v2/{project_id}/exclusive-hosts/{host_id}	workspace:exclusiveHosts:delete	-
GET /v2/{project_id}/market-images	workspace:mkp:listImages	ims:images:list
GET /v2/{project_id}/mkp/commodities/commodity-ids	workspace:mkp:listCommodityInfos	-
POST /v2/{project_id}/mkp/order	workspace:mkp:createOrder	-

API	Action	Dependency
POST /v2/{project_id}/mkp/product-reserve	workspace:mkp:listListProductReserve	-
GET /v2/{project_id}/mkp/commodities	workspace:mkp:listCommodityDetails	-
GET /v2/{project_id}/mkp/commodities/{commodity_id}/relation-commodities	workspace:mkp:listRelationCommodity-Details	-
GET /v2/{project_id}/mkp/commodities/agreements	workspace:mkp:listCommodityAgreements	-
GET /v2/{project_id}/eips	workspace:networks:listEips	• eip:publicIps:list • eip:bandwidths:list
POST /v2/{project_id}/eips	workspace:networks:createEips	• vpc:quotas:list • eip:publicIps:create • eip:publicIps:associateInstance
POST /v2/{project_id}/eips/binding	workspace:networks:bindEips	• eip:publicIps:associateInstance • eip:publicIps:get
POST /v2/{project_id}/eips/unbinding	workspace:networks:unbindEips	• eip:publicIps:list • eip:publicIps:disassociateInstance
GET /v2/{project_id}/eips/quotas	workspace:networks:getEipQuota	vpc:quotas:list
GET /v2/{project_id}/nat-gateways	workspace:networks:ListNatGateways	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/periodic/subscribe/order	workspace:orders:create	• ims:images:list • vpc:vpcs:get • vpc:networks:get • vpc:subnets:get • vpc:ports:get • bss:order:update

API	Action	Dependency
POST /v2/{project_id}/periodic/{desktop_id}/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/change/batch-order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/change/order	workspace:orders:change	• ims:images:list • bss:order:update
POST /v2/{project_id}/desktop-pool/periodic/inquiry/add-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/change-image	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/extend-volume	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/desktop-pool/periodic/inquiry/resize	workspace:orders:batchInquiry	ims:images:list
POST /v2/{project_id}/periodic/inquiry/add-resources	workspace:orders:batchInquiry	ims:images:list
GET /v2/{project_id}/checkOrderLimits	workspace:quotas:check	-
POST /v2/{project_id}/render-desktops	workspace:renderDesktops:create	• ims:images:list • ims:images:share • vpc:networks:get • vpc:ports:create • vpc:ports:delete • vpc:ports:get • vpc:ports:update • vpc:securityGroups:get • vpc:subnets:get • vpc:vpcs:get

API	Action	Dependency
DELETE /v2/{project_id}/render-desktops	workspace:renderDesktops:delete	• vpc:ports:get • vpc:ports:delete
GET /v2/{project_id}/render-desktops	workspace:renderDesktops:list	-
POST /v2/{project_id}/render-desktops/action	workspace:renderDesktops:action	-
GET /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:getFuture	-
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
POST /v2/{project_id}/scheduled-tasks/{task_id}/records/export	workspace:scheduledTasks:exportRecords	-
POST /v2/{project_id}/user/share-resources	workspace:users:subscribeSharer	-
POST /v2/{project_id}/desktop/sub-resources	workspace:desktops:addSubResources	-

API	Action	Dependency
POST /v2/{project_id}/desktop/delete-sub-resources	workspace:desktops:deleteSubResources	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:createSnapshots	-
GET /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:getSnapshots	-
DELETE /v2/{project_id}/desktops/{desktop_id}/snapshots	workspace:desktops:deleteSnapshots	-
POST /v2/{project_id}/desktops/{desktop_id}/snapshots/restore	workspace:desktops:restoreBySnapshot	-
GET /v2/{project_id}/statistics	workspace:statistics:listDesktopStatus	-
GET /v2/{project_id}/desktops/statistics/unused	workspace:statistics:getUnused	-
POST /v2/{project_id}/desktops/statistics/used	workspace:statistics:getUsed	-
GET /v3/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:getConfig	-
POST /v2/{project_id}/terminals/binding-desktops/config	workspace:bindingPolicies:createConfig	-
GET /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:get	-
POST /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:add	-
PUT /v2/{project_id}/terminals/binding-desktops	workspace:bindingPolicies:update	-

API	Action	Dependency
POST /v2/{project_id}/terminals/binding-desktops/batch-delete	workspace:bindingPolicies:delete	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/batch-delete	workspace:volumes:delete	-
POST /v2/{project_id}/volumes	workspace:volumes:batchAdd	-
POST /v2/{project_id}/volumes/expand	workspace:volumes:batchExpand	-
GET /v2/{project_id}/hosts/types	workspace:wdh:getType	-
GET /v2/{project_id}/hosts	workspace:wdh:get	-
GET /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:getRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:createRemoteAssistance	-
DELETE /v2/{project_id}/desktops/{desktop_id}/remote-assistance	workspace:desktops:cancelRemoteAssistance	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes	workspace:volumes:add	-
POST /v2/{project_id}/desktops/{desktop_id}/volumes/{volume_id}/expand	workspace:volumes:expand	-
GET /v2/{project_id}/dss-pools/detail	workspace:volumes:listDssPoolsDetail	dss:pools:list
GET /v2/{project_id}/common/timezones	workspace:common:listTimezones	-
GET /v3/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/images	workspace:images:list	ims:images:list

API	Action	Dependency
POST /v2/{project_id}/policy-groups/import	workspace:policyGroups:import	-
POST /v2/{project_id}/access-policy	workspace:accessPolicies:create	-
GET /v2/{project_id}/access-policy	workspace:accessPolicies:get	-
DELETE /v2/{project_id}/access-policy	workspace:accessPolicies:delete	-
GET /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:getTarget	-
PUT /v2/{project_id}/access-policy/{access_policy_id}/objects	workspace:accessPolicies:updateTarget	-
GET /v2/{project_id}/products	workspace:products:listDesktopProducts	ecs:cloudServerFlavors:get
GET /v2/{project_id}/products/sharer	workspace:products:listSharerProducts	-
GET /v2/{project_id}/products/adninternet	workspace:products:listInternetProducts	-
GET /v2/{project_id}/availability-zones	workspace:availabilityZones:list	-
GET /v2/{project_id}/groups/export	workspace:userGroups:export	-
POST /v3/{project_id}/users/export	workspace:users:export	-
POST /v2/{project_id}/users/import	workspace:users:import	-
GET /v3/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
GET /v2/{project_id}/groups/{group_id}/users/export	workspace:userGroups:exportUsers	-
POST /v2/{project_id}/users/{user_id}/actions	workspace:users:operate	-

API	Action	Dependency
GET /v2/{project_id}/users/{user_id}/random-password	workspace:users:randomPassword	-
DELETE /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:deleteOtps	-
POST /v2/{project_id}/users/{user_id}/resend-email	workspace:users:resendEmail	-
GET /v2/{project_id}/connections/desktops	workspace:connections:securityList	-
GET /v2/{project_id}/connections/desktops/export	workspace:connections:securityExport	-
GET /v2/{project_id}/connections/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/desktops/connections	workspace:connections:securityList	-
GET /v2/{project_id}/desktops/connections/export	workspace:connections:securityExport	-
GET /v2/{project_id}/desktops/online-users	workspace:connections:listOnlineUsers	-
GET /v2/{project_id}/groups	workspace:userGroups:list	-
POST /v2/{project_id}/groups	workspace:userGroups:create	-
POST /v2/{project_id}/groups/batch-delete	workspace:userGroups:batchDelete	-
DELETE /v2/{project_id}/groups/{group_id}	workspace:userGroups:delete	-
PUT /v2/{project_id}/groups/{group_id}	workspace:userGroups:update	-
POST /v2/{project_id}/groups/{group_id}/actions	workspace:userGroups:operate	-
GET /v2/{project_id}/groups/{group_id}/users	workspace:userGroups:getUsers	-

API	Action	Dependency
GET /v2/{project_id}/workspace-sub-jobs	workspace:jobs:listSubJobs	-
POST /v2/{project_id}/workspace-sub-jobs/batch-delete	workspace:jobs:deleteSubJobRecords	-
GET /v2/{project_id}/ous	workspace:ou:get	-
POST /v2/{project_id}/ous	workspace:ou:create	-
DELETE /v2/{project_id}/ous/{ou_id}	workspace:ou:delete	-
PUT /v2/{project_id}/ous/{ou_id}	workspace:ou:update	-
GET /v2/{project_id}/policy-groups	workspace:policyGroups:list	-
POST /v2/{project_id}/policy-groups	workspace:policyGroups:create	-
DELETE /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:delete	-
GET /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:update	-
POST /v2/{project_id}/policy-groups/export	workspace:policyGroups:export	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
PUT /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:updatePolicies	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:listTargets	-

API	Action	Dependency
PUT /v2/{project_id}/policy-groups/{policy_group_id}/targets	workspace:policyGroups:updateTargets	-
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v2/{project_id}/policy-groups/original-policies	workspace:policyGroups:getOriginalPolicies	-
GET /v2/{project_id}/users	workspace:users:list	-
POST /v2/{project_id}/users	workspace:users:create	-
DELETE /v2/{project_id}/users/{user_id}	workspace:users:delete	-
GET /v2/{project_id}/users/{user_id}	workspace:users:get	-
PUT /v2/{project_id}/users/{user_id}	workspace:users:update	-
POST /v2/{project_id}/users/batch-delete	workspace:users:batchDelete	-
POST /v2/{project_id}/users/password	workspace:users:resetPassword	-
POST /v2/{project_id}/users/password-token	workspace:users:checkResetPasswordToken	-
GET /v2/{project_id}/users/desktop-users/template	workspace:users:getTemplate	-
POST /v2/{project_id}/users/exist	workspace:users:checkExist	-
GET /v2/{project_id}/users/{user_id}/otp-devices	workspace:users:listOtps	-
GET /v2/{project_id}/users/template/download	workspace:users:getImportTemplate	-
POST /v2/{project_id}/users/export	workspace:users:export	-

API	Action	Dependency
POST /v2/{project_id}/users/batch-create	workspace:users:batchCreate	-
GET /v2/{project_id}/volume/products	workspace:products:listVolumeProducts	-
GET /v2/{project_id}/export-tasks	workspace:tenants:listExportTasks	-
POST /v2/{project_id}/export-tasks/batch-delete	workspace:tenants:deleteExportTasks	-
GET /v2/{project_id}/export-tasks/{task_id}/download	workspace:tenants:exportData	-
GET /v2/{project_id}/alarms	workspace:statistics:listAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/alarms	workspace:statistics:getAlarm	ces:alarmHistory:list
GET /v2/{project_id}/statistics/growth-rate	workspace:statistics:getGrowthRate	-
GET /v2/{project_id}/statistics/metrics	workspace:statistics:getMetric	-
GET /v2/{project_id}/statistics/metrics/trend	workspace:statistics:getMetricTrend	-
PUT /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:updateNotificationRules	smn:topic:get
DELETE /v2/{project_id}/statistics/notify-rules/{rule_id}	workspace:statistics:deleteNotificationRules	-
POST /v2/{project_id}/statistics/notify-rules	workspace:statistics:createNotifyRules	smn:topic:get
GET /v2/{project_id}/statistics/notify-rules	workspace:statistics:listNotificationRules	-
GET /v2/{project_id}/statistics/notification-records	workspace:statistics:listNotificationRecords	-
GET /v2/{project_id}/statistics/metrics/desktops	workspace:statistics:listDesktopMetrics	-

API	Action	Dependency
GET /v2/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v2/{project_id}/statistics/metrics/users	workspace:statistics:listUserMetrics	-
GET /v2/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
GET /v3/{project_id}/statistics/metrics/desktops/export	workspace:statistics:exportDesktopMetrics	-
GET /v3/{project_id}/statistics/metrics/users/export	workspace:statistics:exportUserMetrics	-
POST /v1/{project_id}/app-center/buckets/actions/create-credential	workspace:appcenter:createBucketCredential	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-center/buckets	workspace:appcenter:createAndAuthorizeBucket	• obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/app-center/apps	workspace:appcenter:listApps	-
POST /v1/{project_id}/app-center/apps	workspace:appcenter:createApp	-
PATCH /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:updateApp	-
DELETE /v1/{project_id}/app-center/apps/{app_id}	workspace:appcenter:deleteApp	-
POST /v1/{project_id}/app-center/apps/{app_id}/actions/auto-install	workspace:appcenter:installApp	-
GET /v1/{project_id}/app-center/apps/{app_id}/authorizations	workspace:appcenter:listAppAuthorizations	-

API	Action	Dependency
POST /v1/{project_id}/app-center/apps/{app_id}/actions/assign-authorizations	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-delete	workspace:appcenter:batchDeleteApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-disable	workspace:appcenter:batchDisableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-enable	workspace:appcenter:batchEnableApps	-
POST /v1/{project_id}/app-center/apps/actions/batch-assign-authorization	workspace:appcenter:batchUpdateAppAuthorizations	-
POST /v1/{project_id}/app-center/apps/actions/batch-auto-install	workspace:appcenter:batchInstallApps	-
GET /v1/{project_id}/app-center/app-catalogs	workspace:appcenter:listAppCatalogs	-
GET /v1/{project_id}/app-center/jobs	workspace:appcenter:listJobs	-
POST /v1/{project_id}/app-center/jobs/actions/batch-delete	workspace:appcenter:batchDeleteJobs	-
POST /v1/{project_id}/app-center/jobs/actions/retry	workspace:appcenter:retryJobs	-
POST /v1/{project_id}/app-center/app-rules	workspace:appcenter:createAppRule	-
GET /v1/{project_id}/app-center/app-rules	workspace:appcenter:listAppRule	-
PATCH /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:updateAppRule	-

API	Action	Dependency
DELETE /v1/{project_id}/app-center/app-rules/{rule_id}	workspace:appcenter:deleteAppRule	-
POST /v1/{project_id}/app-center/app-rules/batch-delete	workspace:appcenter:batchDeleteAppRules	-
POST /v1/{project_id}/app-center/app-rules/actions/enable-rule-restriction	workspace:appcenter:enableRuleRestriction	-
POST /v1/{project_id}/app-center/app-rules/actions/disable-rule-restriction	workspace:appcenter:disableRuleRestriction	-
POST /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:addRestrictedRule	-
GET /v1/{project_id}/app-center/app-restricted-rules	workspace:appcenter:listRestrictedRule	-
POST /v1/{project_id}/app-center/app-restricted-rules/actions/batch-delete	workspace:appcenter:deleteRestrictedRule	-
PATCH /v1/{project_id}/app-center/profiles	workspace:appcenter:updateTenantProfile	-
GET /v1/{project_id}/app-center/profiles	workspace:appcenter:listTenantProfiles	-
POST /v2/{project_id}/scripts	workspace:scripts:create	-
GET /v2/{project_id}/scripts	workspace:scripts:list	-
GET /v2/{project_id}/scripts/{script_id}	workspace:scripts:get	-
PUT /v2/{project_id}/scripts/{script_id}	workspace:scripts:put	-
DELETE /v2/{project_id}/scripts/{script_id}	workspace:scripts:delete	-
POST /v2/{project_id}/script-executions	workspace:scripts:execute	-

API	Action	Dependency
GET /v2/{project_id}/script-execution-records/{record_id}	workspace:scripts:getRecordDetail	-
GET /v2/{project_id}/script-execution-records	workspace:scripts:listRecords	-
GET /v2/{project_id}/script-execution-tasks	workspace:scripts:listTasks	-
POST /v2/{project_id}/script-executions/retry	workspace:scripts:retry	-
POST /v2/{project_id}/script-executions/stop	workspace:scripts:stop	-
POST /v2/{project_id}/script-execution-records/{record_id}/download	workspace:scripts:download	-
GET /v2/{project_id}/share-space/configuration	workspace:tenants:getShareSpaceConfig	-
PUT /v2/{project_id}/share-space/configuration	workspace:tenants:updateShareSpace-Config	-
GET /v2/{project_id}/auth-config/status	workspace:authConfigs:getStatus	-
POST /v2/{project_id}/privacystatement	workspace:privacystatements:sign	-
GET /v2/{project_id}/quotas/detail	workspace:quotas:get	-
GET /v2/{project_id}/sites	workspace:sites:get	-

API	Action	Dependency
POST /v2/{project_id}/sites	workspace:sites:add	• eip:bandwidths:create • eip:publicIps:create • elb:healthmonitors:create • elb:healthmonitors:show • elb:listeners:create • elb:listeners:update • elb:listeners:show • elb:listeners:list • elb:loadbalancers:create • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:list • elb:members:update • elb:pools:create • elb:pools:update • elb:pools:show • vpc:ports:create • vpc:ports:delete • vpc:securityGroupRules:create • vpc:securityGroupRules:delete • vpc:securityGroupRules:get • vpc:securityGroups:create • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:get

API	Action	Dependency
DELETE /v2/{project_id}/sites/{site_id}	workspace:sites:delete	• elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:delete • elb:listeners:show • elb:loadbalancers:delete • elb:loadbalancers:show • elb:members:delete • elb:members:list • elb:pools:delete • elb:pools:show • vpc:ports:delete • vpc:securityGroups:delete • vpcep:endpoints:delete • vpcep:endpoints:get • eip:publicIps:disassociateInstance • eip:bandwidths:delete • eip:publicIps:delete

API	Action	Dependency
PUT /v2/{project_id}/sites/{site_id}/access-mode	workspace:sites:updateAccessMode	• eip:bandwidths:create • eip:bandwidths:delete • eip:publicIps:create • eip:publicIps:delete • eip:publicIps:disassociateInstance • elb:healthmonitors:create • elb:healthmonitors:delete • elb:healthmonitors:show • elb:listeners:create • elb:listeners:delete • elb:listeners:update • elb:listeners:show • elb:loadbalancers:create • elb:loadbalancers:delete • elb:loadbalancers:update • elb:loadbalancers:show • elb:members:create • elb:members:delete • elb:members:list • elb:members:update • elb:pools:create • elb:pools:delete • elb:pools:update • elb:pools:show • vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get • vpcep:endpoints:create • vpcep:endpoints:delete • vpcep:endpoints:get
PUT /v2/{project_id}/sites/{site_id}/subnet-ids	workspace:sites:updateSubnets	• vpc:subnets:get • vpc:subnets:update • vpc:vpcs:get
GET /v2/{project_id}/tenants/lock-status	workspace:tenants:getLockStatus	-
PUT /v2/{project_id}/tenants/lock-status	workspace:tenants:unlock	-

API	Action	Dependency
POST /v2/{project_id}/workspaces/enterprise-ids/check	workspace:tenants:checkEnterpriseIds	-
PUT /v2/{project_id}/workspaces/enterprise-id	workspace:tenants:updateEnterpriseId	-
POST /v2/{project_id}/bandwidths	workspace:bandwidth:create	-
GET /v2/{project_id}/bandwidths	workspace:bandwidth:list	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/update	workspace:bandwidth:update	-
DELETE /v2/{project_id}/bandwidths/{bandwidth_id}	workspace:bandwidth:delete	-
GET /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:getControlConfig	-
PUT /v2/{project_id}/bandwidths/{bandwidth_id}/control-list	workspace:bandwidth:updateControlConfig	-
POST /v2/{project_id}/bandwidths/{bandwidth_id}/periodic/change/order	workspace:bandwidth:createChangeOrder	-
POST /v2/{project_id}/adns	workspace:bandwidth:create	-
GET /v2/{project_id}/adns	workspace:bandwidth:list	-
POST /v2/{project_id}/desktops-adn/batch-delete	workspace:bandwidth:delete	-
POST /v2/{project_id}/snapshots/batch-create	workspace:desktops:batchCreateSnapshots	-

API	Action	Dependency
POST /v2/{project_id}/snapshots/batch-delete	workspace:desktops:batchDeleteSnapshots	-
POST /v2/{project_id}/snapshots/batch-restore	workspace:desktops:batchRestoreSnapshots	-
GET /v2/{project_id}/snapshots	workspace:desktops:listSnapshots	-
POST /v2/{project_id}/verification/desktop-name	workspace:desktops:verifyDesktopName	-
GET /v2/{project_id}/subnets/{subnet_id}/available-ip	workspace:networks:getAvailableIp	-
GET /v2/{project_id}/ad/status	workspace:desktops:getAdStatus	-
GET /v2/{project_id}/ip-exist	workspace:networks:checkIpIfExist	-
POST /v2/{project_id}/desktops/check-images	workspace:images:checkIfExist	ims:images:list
GET /v2/{project_id}/hosts/{host_id}/servers	workspace:wdh:listDesktops	-
PUT /v2/{project_id}/hosts	workspace:wdh:update	-
GET /v2/{project_id}/terminals/binding-desktops/template	workspace:bindingPolicies:getTemplate	-
POST /v2/{project_id}/terminals/binding-desktops/template/import	workspace:bindingPolicies:import	-
GET /v2/{project_id}/terminals/binding-desktops/template/export	workspace:bindingPolicies:export	-
GET /v2/{project_id}/desktops/statistics/run-state	workspace:statistics:getRunState	-
GET /v2/{project_id}/desktops/statistics/login-state	workspace:statistics:getLoginState	-

API	Action	Dependency
GET /v2/{project_id}/subnets/using-subnets	workspace:networks:getUsingSubnets	-
GET /v2/{project_id}/ports	workspace:networks:listPorts	-
GET /v2/{project_id}/render-desktops/{desktop_id}/remote-consoles	workspace:renderDesktops:createConsole	-
PUT /v2/{project_id}/render-desktops/resize	workspace:renderDesktops:resize	-
POST /v2/{project_id}/exclusive-hosts/{host_id}/resize-lites	workspace:exclusiveHosts:resizeLites	-
GET /services/v2/{project_id}/desktops/{desktop_id}	workspace:desktops:get	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktop-monitor/{desktop_id}	workspace:desktops:getMonitor	ces:metricData:get
GET /v2/{project_id}/desktops/export	workspace:desktops:export	• vpc:ports:get • vpc:ports:list • vpc:securityGroups:get • eip:publicIps:list • nat:snatRules:list
GET /v2/{project_id}/desktops/{desktop_id}/detach-info	workspace:desktops:listDetachInfo	-
GET /v2/{project_id}/desktops/{desktop_id}/sysprep	workspace:desktops:getSysprepVersion	-

API	Action	Dependency
POST /v2/{project_id}/internet	workspace:networks:createNat	• vpc:ports:delete • vpc:ports:get • vpc:networks:get • eip:publicIps:create • eip:publicIps:update • eip:publicIps:delete • nat:snatRules:list • nat:snatRules:create • nat:natGateways:list • nat:natGateways:create
GET /v2/{project_id}/internet	workspace:networks:listNats	• vpc:subnets:get • vpc:vpcs:get • nat:snatRules:list • nat:natGateways:list
POST /v2/{project_id}/quotas/check	workspace:quotas:check	-
GET /v2/{project_id}/subnets	workspace:networks:listSubnets	• vpc:subnets:list • vpc:subnets:get
GET /v2/{project_id}/vpcs	workspace:networks:listVpcs	vpc:vpcs:list
POST /v2/{project_id}/policy-groups/policy-template	workspace:policyGroups:createTemplate	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
PUT /v2/{project_id}/policy-groups/policy-template/{policy_group_id}	workspace:policyGroups:updateTemplate	-
GET /v2/{project_id}/security-groups	workspace:networks:listSecurityGroups	-
GET /v2/{project_id}/availability-zones/summary	workspace:availabilityZones:getSummary	-
GET /v2/{project_id}/availability-zones/detail	workspace:availabilityZones:get	-
POST /v2/{project_id}/users/desktop-users/action/import	workspace:users:importUser	-

API	Action	Dependency
POST /v2/{project_id}/users/template-upload	workspace:users:uploadTemplate	-
PUT /v2/{project_id}/access-policy/{access_policy_id}	workspace:accessPolicies:update	-
POST /v2/{project_id}/desktops/{desktop_id}/verify-source	workspace:desktops:verifySource	-
GET /v2/{project_id}/desktops/networks	workspace:desktops:listDesktopNetworks	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:securityGroups:get • eip:publicIps:list
POST /v2/{project_id}/desktops/networks/batch-change	workspace:desktops:batchChangeNetwork	• vpc:vpcs:get • vpc:subnets:get • vpc:networks:get • vpc:ports:get • vpc:ports:create • vpc:ports:update • vpc:ports:delete • vpc:securityGroups:get • eip:publicIps:list • eip:publicIps:associateInstance • eip:publicIps:disassociateInstance
GET /v2/{project_id}/workspace-jobs/{job_id}	workspace:jobs:get	-
POST /v2/{project_id}/ip/import	workspace:accessPolicies:importIp	-
GET /v2/{project_id}/ip/template/download	workspace:accessPolicies:getIpImportTemplate	-
GET /v2/{project_id}/wks-edge-sites	workspace:sites:listEdgeSites	• ies:edgeSite:list • ies:edgeSite:getMetricData
POST /v2/{project_id}/check-edge-site-resources	workspace:sites:checkEdgeSiteResources	• ies:edgeSite:list • ies:edgeSite:getMetricData

API	Action	Dependency
GET /v2/{project_id}/ad-ous	workspace:ou:listAdOus	-
GET /v2/{project_id}/ou-users	workspace:ou:listOuUsers	-
POST /v2/{project_id}/ou-users/import	workspace:ou:importUsersByOU	-
GET /v1/{project_id}/app-groups	workspace:appGroup:list	-
POST /v1/{project_id}/app-groups	workspace:appGroup:create	-
DELETE /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:delete	-
GET /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}	workspace:appGroup:update	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:listPublishedApp	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps	workspace:app:publish	-
GET /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:get	-
PATCH /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}	workspace:app:update	-
DELETE /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:deleteIcon	-

API	Action	Dependency
POST /v1/{project_id}/app-groups/{app_group_id}/apps/{app_id}/icon	workspace:app:uploadIcon	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/check	workspace:app:check	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/disable	workspace:app:batchDisable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/actions/enable	workspace:app:batchEnable	-
POST /v1/{project_id}/app-groups/{app_group_id}/apps/batch-unpublish	workspace:app:unpublish	-
GET /v1/{project_id}/app-groups/{app_group_id}/publishable-app	workspace:appGroup:listPublishableApp	-
POST /v1/{project_id}/app-groups/actions/batch-delete-authorization	workspace:appGroup:batchDeleteAuthorization	-
POST /v1/{project_id}/app-groups/actions/disassociate-app-group	workspace:appGroup:disassociate	-
GET /v1/{project_id}/app-groups/actions/list-authorizations	workspace:appGroup:listAuthorization	-
POST /v1/{project_id}/app-groups/authorizations	workspace:appGroup:addAuthorization	-
POST /v1/{project_id}/app-groups/batch-delete	workspace:appGroup:batchDelete	-
POST /v1/{project_id}/app-groups/rules/validate	workspace:appGroup:check	-

API	Action	Dependency
GET /v1/{project_id}/app-server-groups	workspace:serverGroup:list	-
POST /v1/{project_id}/app-server-groups	workspace:serverGroup:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
DELETE /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:delete	-
GET /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:get	-
PATCH /v1/{project_id}/app-server-groups/{server_group_id}	workspace:serverGroup:update	ims:images:list
GET /v1/{project_id}/app-server-groups/{server_group_id}/state	workspace:serverGroup:getServerState	-
GET /v1/{project_id}/app-server-groups/actions/list	workspace:serverGroup:listDetail	-
GET /v1/{project_id}/app-server-groups/resources/restrict	workspace:serverGroup:getRestrict	-
POST /v1/{project_id}/app-server-groups/rules/validate	workspace:serverGroup:validate	-
POST /v1/{project_id}/server-group/{server_group_id}/tags/create	workspace:serverGroup:tagResource	-
DELETE /v1/{project_id}/server-group/{server_group_id}/tags/delete	workspace:serverGroup:unTagResource	-
GET /v1/{project_id}/server-group/{server_group_id}/tags	workspace:serverGroup:listTagsForResource	-
GET /v1/{project_id}/server-group/tags	workspace:serverGroup:listTags	-

API	Action	Dependency
POST /v1/{project_id}/server-group/tags/batch-create	workspace:serverGroup:batchCreateTags	-
DELETE /v1/{project_id}/server-group/tags/batch-delete	workspace:serverGroup:batchDeleteTags	-
GET /v1/{project_id}/app-servers	workspace:server:list	-
DELETE /v1/{project_id}/app-servers/{server_id}	workspace:server:delete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
GET /v1/{project_id}/app-servers/{server_id}	workspace:server:get	-
PATCH /v1/{project_id}/app-servers/{server_id}	workspace:server:update	-
POST /v1/{project_id}/app-servers/{server_id}/actions/change-image	workspace:server:changeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/{server_id}/actions/reinstall	workspace:server:reinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/app-servers/{server_id}/actions/vnc	workspace:server:getVncUrl	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:list	-
PATCH /v1/{project_id}/app-servers/access-agent/actions/upgrade	workspace:accessAgent:batchUpgrade	-
GET /v1/{project_id}/app-servers/access-agent/latest-version	workspace:accessAgent:listLatestVersion	-
GET /v1/{project_id}/app-servers/access-agent/list	workspace:server:listAccessAgentDetails	-

API	Action	Dependency
GET /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:getUpgradeFlag	-
PATCH /v1/{project_id}/app-servers/access-agent/upgrade-flag	workspace:accessAgent:updateUpgradeFlag	-
GET /v1/{project_id}/app-servers/access-agent/upgrade-record	workspace:accessAgent:listUpgradeRecords	-
POST /v1/{project_id}/app-servers/actions/batch-delete	workspace:server:batchDelete	• iam:roles:listRoles • vpc:ports:delete • vpc:ports:get
PATCH /v1/{project_id}/app-servers/actions/batch-maint	workspace:server:batchChangeMaintainMode	-
PATCH /v1/{project_id}/app-servers/actions/batch-reboot	workspace:server:batchReboot	-
PATCH /v1/{project_id}/app-servers/actions/batch-rejoin-domain	workspace:server:batchRejoinDomain	-
PATCH /v1/{project_id}/app-servers/actions/batch-start	workspace:server:batchStart	-
PATCH /v1/{project_id}/app-servers/actions/batch-stop	workspace:server:batchStop	-
PATCH /v1/{project_id}/app-servers/actions/batch-update-tsvi	workspace:server:batchUpdateTsvi	• vpc:subnets:get • vpc:ports:update

API	Action	Dependency
POST /v1/{project_id}/app-servers/actions/create	workspace:server:create	• ims:images:list • ims:images:updateMemberStatus • ims:images:share • ims:images:get • vpc:securityGroups:get • vpc:securityGroupRules:get • vpc:networks:get • vpc:subnets:get • vpc:ports:create • vpc:ports:get • vpc:ports:delete • vpc:vpcs:get • dss:pools:list
PATCH /v1/{project_id}/app-servers/hosts/batch-migrate	workspace:server:batchMigrateHosts	-
GET /v1/{project_id}/app-servers/metric-data/{server_id}	workspace:server:getMetricData	-
GET /v1/{project_id}/app-server-sub-jobs	workspace:jobs:listSubJobs	-
POST /v1/{project_id}/app-server-sub-jobs/actions/batch-delete	workspace:jobs:batchDeleteSubJobs	-
GET /v1/{project_id}/app-server-sub-jobs/actions/count	workspace:jobs:countSubJobs	-
POST /v1/{project_id}/app-warehouse/action/authorize	workspace:appWarehouse:authorizeObs	• obs:bucket:GetBucketAcl • obs:object:PutObject • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/actions/batch-delete	workspace:appWarehouse:batchDeleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
GET /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:ListWarehouseApps	-
POST /v1/{project_id}/app-warehouse/apps	workspace:appWarehouse:createApp	-

API	Action	Dependency
DELETE /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:deleteApp	• obs:bucket:HeadBucket • obs:object:DeleteObject
POST /v1/{project_id}/app-warehouse/apps/icon	workspace:appWarehouse:uploadAppIcon	obs:object:PutObject
POST /v1/{project_id}/app-warehouse/bucket-and-acl/create	workspace:appWarehouse:createBucketOrAcl	• obs:bucket:GetBucketAcl • obs:bucket:HeadBucket • obs:bucket:PutBucketAcl • obs:bucket:PutReplicationConfiguration • obs:bucket:CreateBucket • obs:bucket:PutBucketCORS
GET /v1/{project_id}/check/quota	workspace:quotas:get	-
GET /v1/{project_id}/image-server-jobs	workspace:images:listImageJobs	-
GET /v1/{project_id}/image-server-jobs/{job_id}	workspace:images:getImageJob	-
GET /v1/{project_id}/image-servers	workspace:imageServer:list	-
POST /v1/{project_id}/image-servers	workspace:imageServer:create	• ims:images:list • vpc:ports:get • vpc:subnets:get
GET /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:get	-
PATCH /v1/{project_id}/image-servers/{server_id}	workspace:imageServer:update	-
POST /v1/{project_id}/image-servers/{server_id}/actions/attach-app	workspace:imageServer:attachApp	-
GET /v1/{project_id}/image-servers/{server_id}/actions/latest-attached-app	workspace:imageServer:listLatestAttachedApp	-

API	Action	Dependency
POST /v1/{project_id}/image-servers/{server_id}/actions/recreate-image	workspace:imageServer:recreate	• vpc:ports:get • vpc:subnets:get • ims:quotas:get • ims:images:get • ims:images:list • ims:images:setTags • ims:images:setOrDeleteTags • ims:images:updateMemberStatus • ims:images:copyInRegion • ims:serverImages:create
PATCH /v1/{project_id}/image-servers/actions/batch-delete	workspace:imageServer:batchDelete	-
GET /v1/{project_id}/image-server-sub-jobs	workspace:imageServer:listImageSubJobs	-
PATCH /v1/{project_id}/image-server-sub-jobs/actions/batch-delete	workspace:imageServer:batchDeleteImageSubJobs	-
GET /v1/{project_id}/image-server-sub-jobs/actions/count	workspace:imageServer:countImageSubJobs	-
GET /v2/{project_id}/job/{job_id}	workspace:jobs:get	-
GET /v1/{project_id}/mails	workspace:appGroup:listMailRecord	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
POST /v1/{project_id}/mails/actions/send	workspace:appGroup:resendMail	-
GET /v1/{project_id}/persistent-storages	workspace:storage:listPersistentStorage	-
POST /v1/{project_id}/persistent-storages	workspace:storage:createPersistentStorage	• obs:bucket:HeadBucket • obs:bucket:PutBucketPolicy • obs:bucket:PutBucketAcl • obs:bucket:PutBucketCORS

API	Action	Dependency
DELETE /v1/{project_id}/persistent-storages/{storage_id}	workspace:storage:deletePersistentStorage	• obs:object:GetObject • obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-folder	workspace:storage:updateUserFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/assign-share-folder	workspace:storage:updateShareFolderAssignment	-
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/create-share-folder	workspace:storage:createShareFolder	• obs:object:GetObject • obs:object:PutObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-storage-claim	workspace:storage:deleteStorageClaim	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/{storage_id}/actions/delete-user-attachment	workspace:storage:deleteUserStorageAttachment	obs:object:DeleteObject
POST /v1/{project_id}/persistent-storages/actions/batch-delete	workspace:storage:batchDeletePersistentStorage	-
GET /v1/{project_id}/persistent-storages/actions/list-attachments	workspace:storage:listStorageAssignment	-
GET /v1/{project_id}/persistent-storages/actions/list-share-folders	workspace:storage:listShareFolder	-
GET /v1/{project_id}/policy-groups/{policy_group_id}	workspace:policyGroups:get	-
GET /v2/{project_id}/policy-groups/{policy_group_id}/policies	workspace:policyGroups:listPolicies	-
GET /v1/{project_id}/policy-groups/{policy_group_id}/target	workspace:policyGroups:listTargets	-

API	Action	Dependency
GET /v2/{project_id}/policy-groups/detail	workspace:policyGroups:listDetail	-
GET /v1/{project_id}/policy-templates	workspace:policyGroups:listTemplate	-
DELETE /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:deleteTemplate	-
PATCH /v1/{project_id}/policy-templates/{policy_template_id}	workspace:policyGroups:updateTemplate	-
GET /v1/{project_id}/privacy-statement	workspace:privacystatements:get	-
DELETE /v1/{project_id}/scaling-policy	workspace:scalingPolicy:delete	-
GET /v1/{project_id}/scaling-policy	workspace:scalingPolicy:list	-
PUT /v1/{project_id}/scaling-policy	workspace:scalingPolicy:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:list	-
POST /v2/{project_id}/scheduled-tasks	workspace:scheduledTasks:create	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records/{record_id}	workspace:scheduledTasks:getRecord	-
DELETE /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:delete	-
POST /v2/{project_id}/scheduled-tasks/future-executions	workspace:scheduledTasks:get	-
PUT /v2/{project_id}/scheduled-tasks/{task_id}	workspace:scheduledTasks:update	-
GET /v2/{project_id}/scheduled-tasks/{task_id}/records	workspace:scheduledTasks:listRecords	-

API	Action	Dependency
POST /v2/{project_id}/scheduled-tasks/batch-delete	workspace:scheduledTasks:batchDelete	-
POST /v1/{project_id}/session/app-connection	workspace:session:listAppConnection	-
POST /v1/{project_id}/session/logoff	workspace:session:logoffUserSession	-
POST /v1/{project_id}/session/user-connection	workspace:session:listUserConnection	-
GET /v1/{project_id}/session/user-session-info	workspace:session:listSessionByUserName	-
PUT /v1/{project_id}/storages-policy/actions/create-statements	workspace:storagePolicy:create	-
GET /v1/{project_id}/storages-policy/actions/list-statements	workspace:storagePolicy:list	-
GET /v2/{project_id}/users	workspace:users:list	-
GET /v1/persistent-storages/actions/list-sfs-storages	workspace:storage:listSfs3Storage	• obs:bucket:ListBucket • obs:bucket:GetBucketStorage • obs:bucket:ListAllMyBuckets
GET /v1/{project_id}/availability-zone	workspace:baseResource:list	ecs:availabilityZones:list
POST /v1/{project_id}/bundles/batch-query-config-info	workspace:tenants:listConfigInfo	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
GET /v1/{project_id}/product	workspace:baseResource:list	-
POST /v1/{project_id}/tenant/action/active	workspace:tenants:active	-
GET /v1/{project_id}/tenant/profile	workspace:tenants:listTenantProfile	-

API	Action	Dependency
GET /v1/{project_id}/volume-type	workspace:baseResource:list	-
GET /v1/{project_id}/app-servers/server-metric-data/{server_id}	workspace:server:listServerMetricData	-
GET /v1/{project_id}/session/list-sessions	workspace:session:listSessions	-
PATCH /v1/{project_id}/app-warehouse/apps/{id}	workspace:appWarehouse:updateApp	-
POST /v1/{project_id}/app-servers/actions/batch-change-image	workspace:server:batchChangeImage	• ims:images:list • vpc:ports:get • vpc:subnets:get
POST /v1/{project_id}/app-servers/actions/batch-reinstall	workspace:server:batchReinstall	• ims:images:list • vpc:ports:get • vpc:subnets:get

Resources

A resource type indicates the resources that an SCP policy applies to. If you specify a resource type for any action in **Table 5-206**, 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 Workspace.

Table 5-206 Resource types supported by Workspace

Resource Type	Description	URN
desktop	Desktop	workspace:<region>:<account-id>:desktop:<desktop-id>
desktopPool	Desktop pool	workspace:<region>:<account-id>:desktopPool:<pool-id>
wdh	Workspace host	workspace:<region>:<account-id>:wdh:<wdh-id>
exclusiveHost	Exclusive host	workspace:<region>:<account-id>:exclusiveHost:<host-id>

Resource Type	Description	URN
user	User	workspace:<region>:<account-id>:user:<user-id>
userGroup	User group	workspace:<region>:<account-id>:userGroup:<group-id>
policyGroup	Policy group	workspace:<region>:<account-id>:policyGroup:<policy-group-id>
script	Script	workspace:<region>:<account-id>:script:<script-id>
scheduledTask	Scheduled task	workspace:<region>:<account-id>:scheduledTask:<task-id>
server	APS	workspace:<region>:<account-id>:server:<server-id>
serverGroup	APS group	workspace:<region>:<account-id>:serverGroup:<server-group-id>
app	Application	workspace:<region>:<account-id>:app:<app-id>
appGroup	Application group	workspace:<region>:<account-id>:appGroup:<app-group-id>
imageServer	Application image server	workspace:<region>:<account-id>:imageServer:<image-server-id>
storage	Storage	workspace:<region>:<account-id>:storage:<storage-id>

Conditions

A Condition element lets you specify conditions for an SCP to take 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, workspace:) only apply to operations of Workspace. For details, see **Table 5-207**.

  - 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 condition value together constitute a complete condition statement. An SCP can be applied only when its request conditions are met. See supported operators.

The following table lists the condition keys that you can define in SCPs for Workspace. You can include these condition keys to specify conditions for an SCP to take effect.

Table 5-207 Service-specific condition keys supported by Workspace

Condition Key	Type	Single-valued/ Multivalued	Description
workspace:AccessMode	string	Multivalued	Access is filtered based on the access mode specified in the request parameter. The valid condition values are **INTERNET**, **DEDICATED**, and **BOTH**.
workspace:CreateOrderType	string	FALSE	Access is filtered based on the created order types specified in the request parameter. The valid condition values are **createDesktops**, **addVolumes**, **createDehHosts**, **rebuildDesktops**, **createDesktopPool**, **expandDesktopPool**, **applyDesktopsInternet**, **createExclusiveHosts**, **subscribeUserSharer**, and **createApps**.

Condition Key	Type	Single-valued/ Multivalued	Description
workspace:ChangeOrderType	string	FALSE	Access is filtered based on the changed order types specified in the request parameter. The valid condition values are **resizeDesktops**, **expandVolumes**, **meteredToPeriod**, **ADD_VOLUME**, **EXTEND_VOLUME**, **RESIZE**, **CHANGE_IMAGE**, **ADD_SUB_RESOURCES**, and **DELETE_SUB_RESOURCES**.
workspace:AssociatePublicIp	boolean	FALSE	Permissions for binding EIPs to desktops are filtered based on whether the associated EIP is enabled.

5.10.13 Management & Governance

5.10.13.1 Simple Message Notification (SMN)

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 SMN, 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 SMN, see **Conditions**.

The following table lists the actions that you can define in SCP statements for SMN.

Table 5-208 Actions supported by SMN

Action	Description	Access Level	Resource Type (*: required)	Condition Key
smn:topic:create	Grants permission to create a topic.	write	topic *	N/A
			N/A	• g:EnterpriseProjectId • g:RequestTag/<tag-key> • g:TagKeys
smn:topic:listTopic	Grants permission to query topics.	list	topic *	N/A
			N/A	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
smn:topic:updateTopic	Grants permission to update a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:get	Grants permission to query details of a topic.	read	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:delete	Grants permission to delete a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:listAttributes	Grants permission to query a topic policy.	list	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:deleteAttribute	Grants permission to delete a topic policy.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:updateAttribute	Grants permission to update a topic policy.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			N/A	• smn:TargetOrgPath • smn:TargetOrgId • smn:TargetAccountId
smn:topic:subscribe	Grants permission to add a subscription to a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			N/A	• smn:Protocol • smn:Endpoint

Action	Description	Access Level	Resource Type (*: required)	Condition Key
smn:topic:listSubscriptionsByTopic	Grants permission to query subscriptions of a topic.	list	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:listSubscriptions	Grants permission to query subscriptions of all topics.	list	topic *	N/A
smn:topic:deleteSubscription	Grants permission to delete a subscription from a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:updateSubscription	Grants permission to update a subscription of a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:publish	Grants permission to publish a message.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:template:create	Grants permission to create a message template.	write	template *	N/A
smn:template:listTemplates	Grants permission to query message templates.	list	template *	N/A
smn:template:update	Grants permission to modify a message template.	write	template *	N/A
smn:template:get	Grants permission to query details of a message template.	read	template *	N/A
smn:template:delete	Grants permission to delete a message template.	write	template *	N/A

Action	Description	Access Level	Resource Type (*: required)	Condition Key
smn:tag:create	Grants permission to add a tag to a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			N/A	• g:RequestTag/<tag-key> • g:TagKeys
smn:tag:delete	Grants permission to delete a tag of a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			N/A	• g:RequestTag/<tag-key> • g:TagKeys
smn:tag:batchModify	Grants permission to batch modify tags of a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
			N/A	• g:RequestTag/<tag-key> • g:TagKeys
smn:tag:list	Grants permission to query tags of a topic.	read	topic *	g:ResourceTag/<tag-key>
smn:topic:createLogTank	Grants permission to associate a topic with a log stream.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:listLogTank	Grants permission to query the log stream associated with a topic.	list	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:updateLogTank	Grants permission to update the log stream associated with a topic.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
smn:topic:deleteLogTank	Grants permission to disassociate a topic from a log stream.	write	topic *	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
smn:topic:createNotifyPolicy	Grants permission to create a notification policy.	write	topic *	N/A
smn:topic:updateNotifyPolicy	Grants permission to modify a notification policy.	write	topic *	N/A
smn:topic:getNotifyPolicy	Grants permission to query a notification policy.	read	topic *	N/A
smn:topic:deleteNotifyPolicy	Grants permission to delete a notification policy.	write	topic *	N/A

Each API of SMN usually supports one or more actions. **Table 5-209** lists the supported actions and dependencies.

Table 5-209 Actions and dependencies supported by SMN APIs

API	Action	Dependencies
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

API	Action	Dependencies
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
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/attributes	smn:topic:deleteAttribute	N/A
PUT /v2/{project_id}/notifications/topics/{topic_urn}/attributes/{name}	smn:topic:updateAttribute	N/A
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/attributes/{name}	smn:topic:deleteAttribute	N/A
POST /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions	smn:topic:subscribe	N/A
GET /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions	smn:topic:listSubscriptionsByTopic	N/A
PUT /v2/{project_id}/notifications/topics/{topic_urn}/subscriptions/{subscription_urn}	smn:topic:updateSubscription	N/A
DELETE /v2/{project_id}/notifications/subscriptions/{subscription_urn}	smn:topic:deleteSubscription	N/A

API	Action	Dependencies
GET /v2/{project_id}/notifications/subscriptions	smn:topic:listSubscriptions	N/A
POST /v2/{project_id}/notifications/topics/{topic_urn}/publish	smn:topic:publish	N/A
POST /v2/{project_id}/notifications/message_template	smn:template:create	N/A
GET /v2/{project_id}/notifications/message_template	smn:template:listTemplates	N/A
PUT /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:update	N/A
GET /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:get	N/A
DELETE /v2/{project_id}/notifications/message_template/{message_template_id}	smn:template:delete	N/A
POST /v2/{project_id}/{resource_type}/{resource_id}/tags	smn:tag:create	N/A
GET /v2/{project_id}/{resource_type}/{resource_id}/tags	smn:tag:list	N/A

API	Action	Dependencies
POST /v2/{project_id}/{resource_type}/{resource_id}/tags/action	smn:tag:batchModify	• smn:tag:create • smn:tag:delete
DELETE /v2/{project_id}/{resource_type}/{resource_id}/tags/{key}	smn:tag:delete	N/A
GET /v2/{project_id}/{resource_type}/tags	smn:tag:list	N/A
POST /v2/{project_id}/{resource_type}/resource_instances/action	smn:tag:list	N/A
GET /v2/{project_id}/notifications/topics/{topic_urn}/logtanks	smn:topic:listLogTank	N/A
POST /v2/{project_id}/notifications/topics/{topic_urn}/logtanks	smn:topic:createLogTank	N/A
PUT /v2/{project_id}/notifications/topics/{topic_urn}/logtanks/{logtank_id}	smn:topic:updateLogTank	N/A
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/logtanks/{logtank_id}	smn:topic:deleteLogTank	N/A

API	Action	Dependencies
POST /v2/{project_id}/notifications/subscriptions/filter_polices	smn:topic:updateSubscription	N/A
PUT /v2/{project_id}/notifications/subscriptions/filter_polices	smn:topic:updateSubscription	N/A
DELETE /v2/{project_id}/notifications/subscriptions/filter_polices	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:listSubscriptionsByTopic
PUT /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id}	smn:topic:updateNotifyPolicy	smn:topic:listSubscriptionsByTopic
GET /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy	smn:topic:getNotifyPolicy	N/A
DELETE /v2/{project_id}/notifications/topics/{topic_urn}/notify-policy/{notify_policy_id}	smn:topic:deleteNotifyPolicy	N/A

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-210**, a 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 SMN.

Table 5-210 Resource types supported by SMN

Resource Type	URN
topic	smn:<region>:<account-id>:topic:<topic-id>
template	smn:<region>:<account-id>:template:<template-id>

Conditions

A Condition element lets you specify conditions for when an SCP is in effect. It contains condition keys and condition 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:**) apply only to operations of the SMN service. For details, see **Table 5-211**.
  - 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.

The following table lists the condition keys that you can define in SCPs for SMN. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-211 Service-specific condition keys supported by SMN

Service-specific Condition Key	Type	Single-valued/ 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.

5.10.13.2 Log Tank Service (LTS)

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 LTS, 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 LTS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for LTS.

Table 5-212 Actions supported by LTS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logGroup:deleteLogGroup	Grants permission to delete a log group.	write	logGroup *	-
lts:logGroup:listLogGroup	Grants permission to query the log group list.	list	-	-
lts:logGroup:createLogGroup	Grants permission to create a log group.	write	-	-
lts:logGroup:updateLogGroup	Grants permission to modify a log group.	write	logGroup *	-
lts:logStream:listLogStream	Grants permission to query the log stream list.	list	logGroup *	-
lts:logStream:deleteLogStream	Grants permission to delete a log stream.	write	logStream *	-
lts:logStream:createLogStream	Grants permission to create a log stream.	write	logGroup *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logStream:searchLog	Grants permission to query logs.	list	logStream *	-
lts:logStream:searchStructLog	Grants permission to query structured logs.	list	logStream *	-
lts:logStream:searchLogHistogram	Grants permission to query the log histogram.	list	logStream *	-
lts:transfer:createTransfer	Grants permission to create a log transfer task.	write	-	-
lts:transfer:deleteTransfer	Grants permission to delete a log transfer task.	write	transfer *	-
lts:transfer:listTransfer	Grants permission to query the log transfer task list.	list	-	-
lts:transfer:updateTransfer	Grants permission to modify a log transfer task.	write	transfer *	-
lts:transfer:registerDmsKafkaInstance	Grants permission to register a DMS Kafka instance.	write	-	-
lts:configCenter:updateOverCollectSwitch	Grants permission to enable or disable log collection beyond free quota.	write	-	-
lts:structConfig:createStructConfig	Grants permission to create structuring configurations.	write	logStream *	-
lts:structConfig:deleteStructConfig	Grants permission to delete structuring configurations.	write	logStream *	-
lts:structConfig:getStructConfig	Grants permission to query structuring configurations.	read	logStream *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:structConfig:listStructTemplate	Grants permission to query the structuring template list.	list	-	-
lts:structConfig:updateStructConfig	Grants permission to modify structuring configurations.	write	logStream *	-
lts:mappingRule:create	Grants permission to create a mapping rule.	write	-	-
lts:mappingRule:delete	Grants permission to delete a mapping rule.	write	-	-
lts:mappingRule:get	Grants permission to query mapping rule details.	read	-	-
lts:mappingRule:list	Grants permission to query the mapping rule list.	list	-	-
lts:mappingRule:update	Grants permission to modify a mapping rule.	write	-	-
lts:logStream:getHistorySql	Grants permission to query historical SQL statements of a log stream.	read	logStream *	-
lts:alarmRule:createSqlAlarmRule	Grants permission to create a SQL alarm rule.	write	-	-
lts:alarmRule:deleteSqlAlarmRule	Grants permission to delete a SQL alarm rule.	write	alarmRule *	-
lts:alarmRule:updateSqlAlarmRule	Grants permission to modify a SQL alarm rule.	write	alarmRule *	-
lts:alarmRule:listSqlAlarmRule	Grants permission to query SQL alarm rules.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:alarmRule:createWordAlarmRule	Grants permission to create a keyword alarm rule.	write	-	-
lts:alarmRule:deleteWordAlarmRule	Grants permission to delete a keyword alarm rule.	write	alarmRule *	-
lts:alarmRule:updateWordAlarmRule	Grants permission to modify a keyword alarm rule.	write	alarmRule *	-
lts:alarmRule:listWordAlarmRule	Grants permission to query keyword alarm rules.	list	-	-
lts:alarm:cleanAlarm	Grants permission to delete an alarm.	write	-	-
lts:alarm:listAlarm	Grants permission to query the alarm list.	list	-	-
lts:logStream:listChart	Grants permission to query log stream charts.	list	-	-
lts:alarmNoticeTemplate:create	Grants permission to create an alarm notification template.	write	-	-
lts:alarmNoticeTemplate:update	Grants permission to modify an alarm notification template.	write	-	-
lts:alarmNoticeTemplate:delete	Grants permission to delete an alarm notification template.	write	-	-
lts:alarmNoticeTemplate:list	Grants permission to query the alarm notification template list.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:alarmNoticeTemplate:get	Grants permission to query alarm notification template details.	read	-	-
lts:hostGroup:create	Grants permission to create a host group.	write	-	-
lts:hostGroup:delete	Grants permission to delete a host group.	write	hostGroup *	-
lts:host:list	Grants permission to query the host list.	list	-	-
lts:hostGroup:list	Grants permission to query the host group list.	list	accessConfig *	-
lts:hostGroup:update	Grants permission to modify a host group.	write	hostGroup *	-
lts:accessConfig:create	Grants permission to create a log ingestion configuration.	write	logStream *	-
lts:accessConfig:delete	Grants permission to delete a log ingestion configuration.	write	accessConfig *	-
lts:accessConfig:list	Grants permission to query log ingestion configurations.	list	-	-
lts:accessConfig:update	Grants permission to modify a log ingestion configuration.	write	accessConfig *	-
			hostGroup	-
lts:tag:create	Grants permission to create a tag.	write	-	-
lts:tag:delete	Grants permission to delete a tag.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logStream:createQuickQuery	Grants permission to create a quick search.	write	logStream *	-
lts:logStream:deleteQuickQuery	Grants permission to delete a quick search.	write	logStream *	-
lts:logStream:listQuickQuery	Grants permission to query quick searches.	list	logGroup *	-
lts:logFavorite:create	Grants permission to add a log to favorites.	write	logStream *	-
lts:logFavorite:delete	Grants permission to remove a log from favorites.	write	-	-
lts:dashboardGroup:create	Grants permission to create a dashboard group.	write	-	-
lts:dashboard:create	Grants permission to create a dashboard.	write	-	-
lts:trafficStatistic:get	Grants permission to query resource statistics details.	read	-	-
lts:tokenizer:get	Grants permission to query configured delimiters.	read	-	-
lts:tokenizer:create	Grants permission to save delimiters.	write	-	-
lts:tokenizer:preview	Grants permission to preview delimiters.	read	-	-
lts:usageAlarm:update	Grants permission to enable or disable quota alarms.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:csvTable:list	Grants permission to query the associated data source configuration table.	list	-	-
lts:csvTable:upload	Grants permission to upload a CSV file.	write	-	-
lts:csvTable:get	Grants permission to preview associated data and query associated data source information.	read	-	-
lts:csvTable:create	Grants permission to create an associated data source.	write	-	-
lts:csvTable:update	Grants permission to update an associated data source.	write	-	-
lts:csvTable:delete	Grants permission to delete an associated data source.	write	-	-
lts:scheduledSql:create	Grants permission to create a SQL scheduled job.	write	-	-
lts:scheduledSql:delete	Grants permission to delete a SQL scheduled job.	write	-	-
lts:scheduledSql:update	Grants permission to modify a SQL scheduled job.	write	-	-
lts:scheduledSql:list	Grants permission to query SQL scheduled jobs.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:scheduledSql:get	Grants permission to query SQL scheduled job details.	read	-	-
lts:scheduledSql:retry	Grants permission to re-execute the instance.	write	-	-
lts:transfer:getDisList	Grants permission to query DIS streams.	list	-	-
lts:transfer:listKafkaInstance	Grants permission to query the Kafka list.	list	-	-
lts:transfer:updateKafkaInstance	Grants permission to update Kafka information.	write	-	-
lts:transfer:deleteKafkaInstance	Grants permission to delete Kafka information.	write	-	-
lts:transfer:listKafkaAuthorization	Grants permission to query the configured Kafka authorization list.	list	-	-
lts:transfer:createKafkaAuthorization	Grants permission to add configured Kafka authorization.	write	-	-
lts:transfer:deleteKafkaAuthorization	Grants permission to delete configured Kafka authorization.	write	-	-
lts:transfer:getTransfer	Grants permission to query transfer task information.	read	transfer *	-
lts:transfer:getDwsInfo	Grants permission to query the DWS information of a tenant.	read	-	-
lts:transfer:registerDwsCluster	Grants permission to register a DMS cluster.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:hostGroup:getHost	Grants permission to query all hosts based on query criteria.	read	-	-
lts:hostGroup:get	Grants permission to query all configurations of a host group based on query criteria.	read	-	-
lts:accessConfig:get	Grants permission to query a collection configuration.	read	accessConfig *	-
lts:logFavorite:list	Grants permission to query the favorites list.	list	-	-
lts:logFavorite:update	Grants permission to modify favorites.	write	logStream *	-
lts:logGroup:getLogGroup	Grants permission to query a log group.	read	logGroup *	-
lts:IndexConfig:list	Grants permission to query indexes.	list	logGroup *	-
lts:IndexConfig:create	Grants permission to create an index.	write	logGroup *	-
lts:structConfig:listStructConfig	Grants permission to query log stream structuring information.	list	logStream *	-
lts:logStream:updateLogStream	Grants permission to modify a log stream.	write	logStream *	-
lts:logStream:getRealtimeLog	Grants permission to query real-time logs.	read	logStream *	-
lts:logStream:getLogStream	Grants permission to query log stream information.	read	logStream *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logStream:createLogFilterRules	Grants permission to create a log cleaning rule.	write	logStream *	-
lts:logStream:updateLogFilterRules	Grants permission to modify a log cleaning rule.	write	logStream *	-
lts:logStream:deleteLogFilterRules	Grants permission to delete a log cleaning rule.	write	logStream *	-
lts:logStream:listLogFilterRules	Grants permission to query log cleaning rules.	list	logStream *	-
lts:logStream:getQuickQuery	Grants permission to query a quick search.	list	logStream *	-
lts:logStream:updateQuickQuery	Grants permission to modify a quick search.	write	logStream *	-
lts:logStream:searchLogContext	Grants permission to query log context.	read	logStream *	-
lts:structConfig:getCustomTemplate	Grants permission to query a custom template.	read	-	-
lts:structConfig:createCustomTemplate	Grants permission to create a custom template.	write	-	-
lts:structConfig:updateCustomTemplate	Grants permission to modify a custom template.	write	-	-
lts:structConfig:deleteCustomTemplate	Grants permission to delete a custom template.	write	-	-
lts:structConfig:listCustomTemplate	Grants permission to query the custom template list.	read	-	-
lts:structConfig:smartExtra	Grants permission to intelligently extract structured fields.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logStream:getAggrResult	Grants permission to query quick analysis results.	read	logStream *	-
lts:logStream:getAggr	Grants permission to query a quick analysis aggregator.	read	-	-
lts:logStream:createAggr	Grants permission to create a quick analysis aggregator.	write	-	-
lts:logStream:deleteAggr	Grants permission to delete a quick analysis aggregator.	write	-	-
lts:logStream:getQuickAnalysisAggValue	Grants permission to query quick analysis results of numeric types.	read	logStream *	-
lts:logStream:getWordFreqConfig	Grants permission to query the quick analysis fields created by a user.	read	logStream *	-
lts:logStream:refreshWordFreqConfig	Grants permission to modify a quick analysis field.	write	logStream *	-
lts:logCrux:list	Grants permission to query LogReduce information.	list	-	-
lts:logCrux:get	Grants permission to query the LogReduce switch status.	read	-	-
lts:logCrux:enable	Grants permission to enable LogReduce.	write	-	-
lts:logCrux:disable	Grants permission to disable LogReduce.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logStream:updateChart	Grants permission to update a user log statistical chart.	write	-	-
lts:logStream:createChart	Grants permission to create a user log statistical chart.	write	-	-
lts:logStream:deleteChart	Grants permission to delete a user log statistical chart.	write	logStream *	-
lts:logStream:getChart	Grants permission to query a user log statistical chart.	read	logStream *	-
lts:dashboard:deleteChart	Grants permission to delete a chart.	write	dashboard *	-
lts:dashboard:listCharts	Grants permission to display dashboard-level charts.	list	-	-
lts:dashboard:updateChart	Grants permission to move a chart.	write	dashboard *	-
lts:dashboard:getDashboard	Grants permission to query a user log dashboard.	read	-	-
lts:dashboardGroup:getDashboardsGroup	Grants permission to query a user log dashboard group.	read	-	-
lts:dashboardGroup:updateDashboardsGroup	Grants permission to modify a user log dashboard group.	write	-	-
lts:dashboardGroup:deleteDashboardsGroup	Grants permission to update a user log dashboard group.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:dashboard:CreateDashBoard	Grants permission to create dashboards in batches based on a log dashboard template.	write	-	-
lts:dashboard:CreateDashBoardTemplate	Grants permission to create a user log dashboard template.	write	-	-
lts:dashboard:getDashBoardTemplate	Grants permission to query a user log dashboard template.	read	-	-
lts:dashboard:updateDashBoardTemplate	Grants permission to modify a user log dashboard template.	write	-	-
lts:dashboard:deleteDashBoardTemplate	Grants permission to delete a user log dashboard template.	write	-	-
lts:dashboardGroup:createLogDashboardTemplateGroup	Grants permission to create a dashboard template group.	write	-	-
lts:dashboardGroup:updateLogDashboardTemplateGroup	Grants permission to modify a dashboard template group.	write	-	-
lts:dashboardGroup:deleteLogDashboardTemplateGroup	Grants permission to delete a user log dashboard template group.	write	-	-
lts:dashboard:listFilter	Grants permission to query dashboard filters.	list	dashboard *	-
lts:dashboard:createFilter	Grants permission to create a dashboard filter.	write	dashboard *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:dashboard:updateFilter	Grants permission to modify a dashboard filter.	write	dashboard *	-
lts:dashboard:deleteFilter	Grants permission to delete a dashboard filter.	write	dashboard *	-
lts:alarmRule:listAlarmRules	Grants permission to query the alarm rule list.	list	-	-
lts:alarmRule:getKeywordsAlarmRule	Grants permission to query a keyword alarm rule.	read	alarmRule *	-
lts:alarmRule:getSqlAlarmRule	Grants permission to query a SQL alarm rule.	read	alarmRule *	-
lts:alarm:listAlarmStatistic	Grants permission to query SQL alarm data.	list	-	-
lts:dashboard:update	Grants permission to modify a user log dashboard.	write	-	-
lts:dashboard:delete	Grants permission to delete a user log dashboard.	write	-	-
lts:logSearch:list	Grants permission to obtain the cluster, namespace, component, instance, log, node, log file page component, and file lists.	list	-	-
lts:logSearch:getTime	Grants permission to query the current time of a backend node.	read	-	-
lts:logSearch:getLogContext	Grants permission to obtain log context.	read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logSearch:exportLogs	Grants permission to download logs.	write	-	-
lts:ageingTime:get	Grants permission to obtain quota management.	list	-	-
lts:ageingTime:update	Grants permission to modify quota management.	write	-	-
lts:logConfigPath:list	Grants permission to query VM log path configurations.	list	-	-
lts:logConfigPath:create	Grants permission to create a VM log path configuration.	write	-	-
lts:structRule:get	Grants permission to obtain a structuring rule.	read	-	-
lts:structRule:create	Grants permission to create a structuring rule.	write	-	-
lts:structRule:delete	Grants permission to delete a structuring rule.	write	-	-
lts:structRule:regex	Grants permission to extract data in a structured manner.	write	-	-
lts:logPail:list	Grants permission to query log buckets, logs in buckets, and log bar charts.	list	-	-
lts:structSql:list	Grants permission to query structured logs.	list	-	-
lts:logPail:create	Grants permission to add a log bucket.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logPail:update	Grants permission to modify a log bucket.	list	-	-
lts:logPail:delete	Grants permission to delete a log bucket.	write	-	-
lts:storageRelation:list	Grants permission to query transfer relationships of the current tenant.	list	-	-
lts:storageRelation:delete	Grants permission to delete transfer relationships of the current tenant.	write	-	-
lts:storage:batchAction	Grants permission to periodically start and stop tasks in batches.	write	-	-
lts:logPailDump:create	Grants permission to add a log transfer task.	write	-	-
lts:statisticsRule:list	Grants permission to query a statistical rule.	list	-	-
lts:statisticsRule:create	Grants permission to create a statistical rule.	write	-	-
lts:statisticsRule:update	Grants permission to modify a statistical rule.	write	-	-
lts:statisticsRule:delete	Grants permission to delete a statistical rule.	write	-	-
lts:transfer:listKafkaInstanceTopic	Grants permission to query all topics of a Kafka instance.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logPackage:create	Grants permission to purchase resource packages.	write	-	-
lts:consumerGroup:create	Grants permission to create a consumer group.	write	-	-
lts:consumerGroup:delete	Grants permission to delete a consumer group.	write	-	-
lts:consumerGroup:list	Grants permission to query the consumer group list.	list	-	-
lts:consumerGroup:get	Grants permission to query the consumer group details.	read	-	-
lts:consumerGroup:update	Grants permission to modify a consumer group.	write	-	-
lts:logStream:get	Grants permission to obtain log stream details.	read	-	-
lts:agency:listGroupAndStream	Grants permission to obtain the log stream list of the delegator's log group.	list	-	-
lts:agency:listEps	Grants permission to obtain the EPS list of the delegator.	list	-	-
lts:agency:listStructConfig	Grants permission to obtain the structuring configurations of the delegator.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:logConverge:get	Grants permission to obtain the multi-account log center configurations.	read	-	-
lts:logConverge:update	Grants permission to update the multi-account log center configurations.	write	-	-
lts:logManager:createAggr	Grants permission to create a quick analysis aggregator.	write	logStream *	-
lts:logManager:createAggrs	Grants permission to create quick analysis aggregators in batches.	write	logStream *	-
lts:logManager:deleteAggr	Grants permission to delete a quick analysis aggregator.	write	logStream *	-
lts:logManager:deleteAggrs	Grants permission to delete quick analysis aggregators in batches.	write	logStream *	-
lts:logmanager:createLogFilter	Grants permission to create a log cleaning rule.	write	logStream *	-
lts:logmanager:listLogFilters	Grants permission to query a log cleaning rule.	read	logStream *	-
lts:logmanager:updateLogFilters	Grants permission to modify a log cleaning rule.	write	logStream *	-
lts:logmanager:deleteLogFilters	Grants permission to delete a log cleaning rule.	write	logStream *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
lts:structConfig:regex	Grants permission to structure the example log using regular expressions.	write	-	-

Each API of LTS usually supports one or more actions. **Table 5-213** lists the supported actions and dependencies.

Table 5-213 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	-
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	-

API	Action	Dependencies
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	-
POST /v2/{project_id}/streams/{log_stream_id}/struct-content/query	lts:logStream:searchStructLog	-
POST /v2/{project_id}/log-dump/obs	lts:transfer:createTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:HeadBucket
POST /v2/{project_id}/transfers	lts:transfer:createTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:GetEncryptionConfiguration • obs:bucket:HeadBucket • dis:streams:list • dis:streamPolicies:list
DELETE /v2/{project_id}/transfers	lts:transfer:deleteTransfer	-
GET /v2/{project_id}/transfers	lts:transfer:listTransfer	-

API	Action	Dependencies
POST /v2/{project_id}/lts/dms/kafka-instance	lts:transfer:registerDmsKafkaInstance	dms:instance:list
PUT /v2/{project_id}/transfers	lts:transfer:updateTransfer	• obs:bucket:PutBucketAcl • obs:bucket:GetBucketAcl • obs:bucket:GetEncryptionConfiguration • obs:bucket:HeadBucket • dis:streams:list • dis:streamPolicies:list
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	-
POST /v2/{project_id}/lts/struct/template	lts:structConfig:createStructConfig	-
DELETE /v2/{project_id}/lts/struct/template	lts:structConfig:deleteStructConfig	-
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	-

API	Action	Dependencies
PUT /v2/{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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
POST /v3/{project_id}/lts/host-list	lts:host:list	• aom:icmgr:get • aom:icmgr:list
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-214**, 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 LTS.

Table 5-214 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>
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 SCPs. It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.13.3 Identity and Access Management (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.

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 IAM, 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 IAM, see **Conditions**.

The following table lists the actions that you can define in SCP statements for IAM. The actions without the V5 suffix are used to control access to the old IAM console, and the actions with the V5 suffix are used to control access to the new IAM console.

Table 5-215 Actions supported by IAM

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam::listAccessKeys	Grants permission to list permanent access keys.	List	-	-
iam::createAccessKey	Grants permission to create a permanent access key.	Write	-	-
iam::getAccessKey	Grants permission to query a permanent access key.	Read	-	-
iam::updateAccessKey	Grants permission to update a permanent access key.	Write	-	-
iam::deleteAccessKey	Grants permission to delete a permanent access key.	Write	-	-
iam:projects:list	Grants permission to list projects.	List	-	-
iam:projects:create	Grants permission to create a project.	Write	-	-
iam:projects:listForUser	Grants permission to list projects of a specified user.	List	-	-
iam:projects:update	Grants permission to update a project.	Write	-	-
iam:groups:list	Grants permission to list groups.	List	-	-
iam:groups:create	Grants permission to create a group.	Write	-	-
iam:groups:get	Grants permission to query a group.	Read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:groups:delete	Grants permission to delete a group.	Write	-	-
iam:groups:update	Grants permission to update a group.	Write	-	-
iam:groups:removeUser	Grants permission to remove a user from a group.	Write	-	-
iam:groups:listUsers	Grants permission to list users of a specified group.	List	-	-
iam:groups:checkUser	Grants permission to query whether a user is in the group.	Read	-	-
iam:groups:addUser	Grants permission to add a user to a group.	Write	-	-
iam:users:create	Grants permission to create a user.	Write	-	-
iam:users:get	Grants permission to query a user.	Read	-	-
iam:users:update	Grants permission to update a user.	Write	-	-
iam:users:list	Grants permission to list users.	List	-	-
iam:users:delete	Grants permission to delete a user.	Write	-	-
iam:users:listGroups	Grants permission to list groups of a specified user.	List	-	-
iam:users:listVirtualMFADevices	Grants permission to list virtual MFA devices of a specified user.	List	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:users:createVirtualMFADevice	Grants permission to create a secret key for a virtual MFA device.	Write	-	-
iam:users:deleteVirtualMFADevice	Grants permission to delete a virtual MFA device.	Write	-	-
iam:users:getVirtualMFADevice	Grants permission to query a virtual MFA device.	Read	-	-
iam:users:bindVirtualMFADevice	Grants permission to bind a virtual MFA device.	Write	-	-
iam:users:unbindVirtualMFADevice	Grants permission to unbind a virtual MFA device.	Write	-	-
iam:identityProviders:list	Grants permission to list identity providers.	List	-	-
iam:identityProviders:get	Grants permission to query an identity provider.	Read	-	-
iam:identityProviders:create	Grants permission to create an identity provider.	Write	-	-
iam:identityProviders:delete	Grants permission to delete an identity provider.	Write	-	-
iam:identityProviders:update	Grants permission to update an identity provider.	Write	-	-
iam:identityProviders:listMappings	Grants permission to list mappings of an identity provider.	List	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:identityProviders:getMapping	Grants permission to query a mapping of an identity provider.	Read	-	-
iam:identityProviders:createMapping	Grants permission to create a mapping for an identity provider.	Write	-	-
iam:identityProviders:deleteMapping	Grants permission to delete a mapping of an identity provider.	Write	-	-
iam:identityProviders:updateMapping	Grants permission to update a 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 a protocol of an identity provider.	Read	-	-
iam:identityProviders:createProtocol	Grants permission to create a protocol for an identity provider.	Write	-	-
iam:identityProviders:deleteProtocol	Grants permission to delete a 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
iam:identityProviders:getSAMLMetadata	Grants permission to query a SAML metadata file of an identity provider.	Read	-	-
iam:identityProviders:createSAMLMetadata	Grants permission to create a SAML metadata file for an identity provider.	Write	-	-
iam:identityProviders:getOIDCConfig	Grants permission to query the OIDC configuration of an identity provider.	Read	-	-
iam:identityProviders:createOIDCConfig	Grants permission to create the OIDC configuration of an identity provider.	Write	-	-
iam:identityProviders:updateOIDCConfig	Grants permission to update the OIDC configuration of an identity provider.	Write	-	-
iam:securityPolicies:getProtectPolicy	Grants permission to query an operation protection policy.	Read	-	-
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	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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 update a console access policy.	Write	-	-
iam:securityPolicies:getApiAclPolicy	Grants permission to query an API access policy.	Read	-	-
iam:securityPolicies:updateApiAclPolicy	Grants permission to update an API access policy.	Write	-	-
iam:users:listLoginProtectSettings	Grants permission to list user login protection settings under a tenant.	List	-	-
iam:users:getLoginProtectSetting	Grants permission to query login protection settings.	Read	-	-
iam:users:updateLoginProtectSetting	Grants permission to update login protection settings.	Write	-	-
iam:quotas:list	Grants permission to list quotas.	List	-	-
iam:quotas:listForProject	Grants permission to list quotas of a specified project.	List	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:agencies:pass	Grants permission to pass an agency to a cloud service.	Permission_management	agency *	-
iam:roles:list	Grants permission to query a permission list.	List	-	-
iam:roles:get	Grants permission to query permission details.	Read	-	-
iam::listRoleAssignments	Grants permission to query authorization records of a tenant.	List	-	-
iam:groups:listRolesOnDomain	Grants permission to query group permissions in global services.	List	-	-
iam:groups:listRolesOnProject	Grants permission to query group permissions in project services.	List	-	-
iam:groups:grantRoleOnDomain	Grants permission to grant global service permissions to a group.	Write	-	-
iam:groups:grantRoleOnProject	Grants permission to grant project service permissions to a group.	Write	-	-
iam:groups:checkRoleOnDomain	Grants permission to query whether a group has global service permissions.	Read	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:groups:checkRoleOnProject	Grants permission to query whether a group has project service permissions.	Read	-	-
iam:groups:listRoles	Grants permission to query permissions of a group.	List	-	-
iam:groups:checkRole	Grants permission to query whether a group has specified permissions.	Read	-	-
iam:groups:revokeRole	Grants permission to remove specified permissions from a group.	Write	-	-
iam:groups:revokeRoleOnDomain	Grants permission to remove global service permissions from a group.	Write	-	-
iam:groups:revokeRoleOnProject	Grants permission to remove project service permissions from a group.	Write	-	-
iam:groups:grantRole	Grants permission to grant specified permissions to a group.	Write	-	-
iam:roles:create	Grants permission to create a custom policy.	Write	-	-
iam:roles:update	Grants permission to update a custom policy.	Write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:roles:delete	Grants permission to delete a custom policy.	Write	-	-
iam:agencies:list	Grants permission to list agencies.	List	-	-
iam:agencies:get	Grants permission to query details of a specified agency.	Read	-	-
iam:agencies:create	Grants permission to create an agency.	Write	-	-
iam:agencies:update	Grants permission to update an agency.	Write	-	-
iam:agencies:delete	Grants permission to delete an agency.	Write	-	-
iam:agencies:listRolesOnDomain	Grants permission to query global service permissions of an agency.	List	-	-
iam:agencies:listRolesOnProject	Grants permission to query the permissions of a specified project for an agency.	List	-	-
iam:agencies:grantRoleOnDomain	Grants permission to grant global service permissions to an agency.	Write	-	-
iam:agencies:grantRoleOnProject	Grants permission to grant project service permissions to an agency.	Write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:agencies:checkRoleOnDomain	Grants permission to query whether an agency has global service permissions.	Read	-	-
iam:agencies:checkRoleOnProject	Grants permission to query whether an agency has project service permissions.	Read	-	-
iam:agencies:revokeRoleOnDomain	Grants permission to remove global service permissions from an agency.	Write	-	-
iam:agencies:revokeRoleOnProject	Grants permission to remove project service permissions from an agency.	Write	-	-
iam:agencies:listRoles	Grants permission to query permissions of an agency.	List	-	-
iam:agencies:grantRole	Grants permission to grant specified permissions to an agency.	Write	-	-
iam:agencies:checkRole	Grants permission to query whether an agency has specified permissions.	Read	-	-
iam:agencies:revokeRole	Grants permission to remove specified permissions from an agency.	Write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam::listGroupsAssignedEnterprise-Project	Grants permission to query permissions of a group associated with an enterprise project.	List	-	-
iam:groups:listRolesOnEnterpriseProject	Grants permission to query permissions of a group associated with an enterprise project.	List	-	-
iam:groups:grantRoleOnEnterprise-Project	Grants permission to grant permissions to an enterprise project based on groups.	Write	-	-
iam:groups:revokeRoleOnEnterprise-Project	Grants permission to delete permissions of a group associated with an enterprise project.	Write	-	-
iam:groups:listAssignedEnterpriseProjects	Grants permission to query enterprise projects associated with a group.	List	-	-
iam:users:listAssignedEnterprisePro-jects	Grants permission to query enterprise projects associated with a user.	List	-	-
iam::listUsersAssignedEnterprisePro-ject	Grants permission to query users associated with an enterprise project.	List	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:users:listRolesOnEnterpriseProject	Grants permission to query permissions of a user associated with an enterprise project.	List	-	-
iam:users:grantRoleOnEnterpriseProject	Grants permission to grant permissions to an enterprise project based on users.	Write	-	-
iam:users:revokeRoleOnEnterpriseProject	Grants permission to delete permissions of a user associated with an enterprise project.	Write	-	-
iam:agencies:grantRoleOnEnterpriseProject	Grants permission to grant permissions to an enterprise project based on agencies.	Write	-	-
iam:agencies:revokeRoleOnEnterpriseProject	Grants permission to delete permissions of an agency associated with an enterprise project.	Write	-	-
iam:mfa:listVirtualMFADevicesV5	Grants permission to list virtual MFA devices.	List	mfa *	-
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 virtual MFA device.	Write	mfa *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:mfa:disableV5	Grants permission to disable a virtual MFA device.	Write	mfa *	-
iam:securitypolicies:getPasswordPolicyV5	Grants permission to obtain password policy information.	Read	-	-
iam:securitypolicies:updatePasswordPolicyV5	Grants permission to update a password policy.	Write	-	-
iam:securitypolicies:getLoginPolicyV5	Grants permission to obtain login policy information.	Read	-	-
iam:securitypolicies:updateLoginPolicyV5	Grants permission to update a login policy.	Write	-	-
iam:credentials:listCredentialsV5	Grants permission to list permanent access keys for an IAM user.	List	user *	g:ResourceTag/<tag-key>
iam:credentials:showAccessKeyLastUsedV5	Grants permission to obtain the last usage time of a specified permanent access key.	Read	user *	g:ResourceTag/<tag-key>
iam:credentials:createCredentialV5	Grants permission to create a permanent access key for an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:credentials:updateCredentialV5	Grants permission to update a permanent access key for an IAM user.	Write	user *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:credentials:deleteCredentialV5	Grants permission to delete a permanent access key for an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:users:changePasswordV5	Grants permission to change their own passwords for an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:users:showLoginProfileV5	Grants permission to obtain login information of an IAM user.	Read	user *	g:ResourceTag/<tag-key>
iam:users:createLoginProfileV5	Grants permission to create login information for an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:users:updateLoginProfileV5	Grants permission to update login information for an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:users:deleteLoginProfileV5	Grants permission to delete login information for an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:users:listUsersV5	Grants permission to list IAM users.	List	user *	-
iam:users:getUserV5	Grants permission to obtain information of an IAM user.	Read	user *	g:ResourceTag/<tag-key>
iam:users:showUserLastLoginV5	Grants permission to obtain the last login time of an IAM user.	Read	user *	g:ResourceTag/<tag-key>
iam:users:createUserV5	Grants permission to create an IAM user.	Write	user *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:users:updateUserV5	Grants permission to update an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:users:deleteUserV5	Grants permission to delete an IAM user.	Write	user *	g:ResourceTag/<tag-key>
iam:groups:listGroupsV5	Grants permission to list groups.	List	group *	-
iam:groups:getGroupV5	Grants permission to obtain group information.	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 *	-
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 obtain identity policy information.	Read	policy *	-
iam:policies:createV5	Grants permission to create a custom identity policy.	Permission_management	policy *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:policies:deleteV5	Grants permission to delete a custom identity policy.	Permission_management	policy *	-
iam:policies:listVersionsV5	Grants permission to list identity policy versions.	List	policy *	-
iam:policies:getVersionV5	Grants permission to obtain identity policy version information.	Read	policy *	-
iam:policies:createVersionV5	Grants permission to create another 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 the default version for a custom identity policy.	Permission_management	policy *	-
iam:agencies:attachPolicyV5	Grants permission to attach an identity policy to an agency or trust agency.	Permission_management	agency *	g:ResourceTag/<tag-key>
			-	**iam:PolicyURN**
iam:groups:attachPolicyV5	Grants permission to attach an identity policy to a group.	Permission_management	group *	-
			-	**iam:PolicyURN**
iam:users:attachPolicyV5	Grants permission to attach an identity policy to an IAM user.	Permission_management	user *	g:ResourceTag/<tag-key>
			-	**iam:PolicyURN**

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:agencies:detachPolicyV5	Grants permission to detach an identity policy from an agency or trust agency.	Permission_management	agency *	g:ResourceTag/<tag-key>
			-	**iam:PolicyURN**
iam:groups:detachPolicyV5	Grants permission to detach an identity policy from a group.	Permission_management	group *	-
			-	**iam:PolicyURN**
iam:users:detachPolicyV5	Grants permission to detach an identity policy from an IAM user.	Permission_management	user *	g:ResourceTag/<tag-key>
			-	**iam:PolicyURN**
iam:policies:listEntitiesV5	Grants permission to list all entities attached to an identity policy.	List	policy *	-
iam:agencies:listAttachedPoliciesV5	Grants permission to list the identity policies attached to an agency or trust agency.	List	agency *	g:ResourceTag/<tag-key>
iam:groups:listAttachedPoliciesV5	Grants permission to list the identity policies attached to a group.	List	group *	-
iam:users:listAttachedPoliciesV5	Grants permission to list the identity policies attached to an IAM user.	List	user *	g:ResourceTag/<tag-key>
iam:agencies:createServiceLinkedAgencyV5	Grants permission to create a service-linked agency to allow the cloud service to perform operations on your behalf.	Write	agency *	-
			-	**iam:ServicePrincipal**

Action	Description	Access Level	Resource Type (*: required)	Condition Key
iam:agencies:deleteServiceLinkedAgencyV5	Grants permission to delete a service-linked agency.	Write	agency *	g:ResourceTag/<tag-key>
			-	iam:ServicePrincipal
iam:agencies:getServiceLinkedAgencyDeletionStatusV5	Grants permission to obtain the 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 obtain agencies and trust agencies.	Read	agency *	g:ResourceTag/<tag-key>
iam:agencies:createV5	Grants permission to create a trust agency.	Write	agency *	-
iam:agencies:updateV5	Grants permission to update a trust agency.	Write	agency *	g:ResourceTag/<tag-key>
iam:agencies:deleteV5	Grants permission to delete a trust agency.	Write	agency *	g:ResourceTag/<tag-key>
iam:agencies:updateTrustPolicyV5	Grants permission to update the trust policy of a trust agency.	Write	agency *	g:ResourceTag/<tag-key>
iam::listTagsForResourceV5	Grants permission to list resource tags.	List	agency	g:ResourceTag/<tag-key>
			user	g:ResourceTag/<tag-key>
iam::tagForResourceV5	Grants permission to set resource tags.	Tagging	agency	g:ResourceTag/<tag-key>
			user	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			-	• g:RequestTag/<tag-key> • g:TagKeys
iam::untagForResourceV5	Grants permission to delete resource tags.	Tagging	agency	g:ResourceTag/<tag-key>
			user	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
iam::getAccountSummaryV5	Grants permission to obtain the IAM entity usage and IAM quotas of an account.	List	-	-
iam::getAsymmetricSignatureSwitchV5	Grants permission to obtain the asymmetric signature switch status of a temporary token.	Read	-	-
iam::setAsymmetricSignatureSwitchV5	Grants permission to set the asymmetric signature switch status of a temporary token.	Write	-	-

Each API of IAM usually supports one or more actions. **Table 5-216** lists the supported actions and dependencies.

Table 5-216 Actions and dependencies supported by IAM APIs

API	Action	Dependencies
GET /v3.0/OS-CREDENTIAL/credentials	iam::listAccessKeys	-
POST /v3.0/OS-CREDENTIAL/credentials	iam::createAccessKey	-

API	Action	Dependencies
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	-
PUT /v3/groups/{group_id}/users/{user_id}	iam:groups:addUser	-

API	Action	Dependencies
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:listVirtualMFADevices	-
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:getVirtualMFADevice	-
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:listLoginProtectSettings	-
GET /v3.0/OS-USER/users/{user_id}/login-protect	iam:users:getLoginProtectSetting	-

API	Action	Dependencies
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	-
GET /v3/OS-FEDERATION/identity_providers/{idp_id}/protocols/{protocol_id}	iam:identityProviders:getProtocol	-

API	Action	Dependencies
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	-
GET /v3.0/OS-SECURITYPOLICY/domains/{domain_id}/protect-policy	iam:securityPolicies:getProtectPolicy	-

API	Action	Dependencies
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	-
GET /v3.0/OS-PERMISSION/role-assignments	iam::listRoleAssignments	-

API	Action	Dependencies
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	-

API	Action	Dependencies
DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}	iam:groups:revokeRoleOnProject	-
PUT /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects	iam:groups:grantRole	-
GET /v3.0/OS-ROLE/roles	iam:roles:list	-
GET /v3.0/OS-ROLE/roles/{role_id}	iam:roles:get	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
POST /v3.0/OS-ROLE/roles	iam:roles:create	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
PATCH /v3.0/OS-ROLE/roles/{role_id}	iam:roles:update	-
DELETE /v3.0/OS-ROLE/roles/{role_id}	iam:roles:delete	-
GET /v3.0/OS-AGENCY/agencies	iam:agencies:list	-
GET /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:get	-
POST /v3.0/OS-AGENCY/agencies	iam:agencies:create	-
PUT /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:update	-
DELETE /v3.0/OS-AGENCY/agencies/{agency_id}	iam:agencies:delete	-
GET /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnDomain	-

API	Action	Dependencies
GET /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles	iam:agencies:listRolesOnProject	-
PUT /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnDomain	-
PUT /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:grantRoleOnProject	-
HEAD /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnDomain	-
HEAD /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:checkRoleOnProject	-
DELETE /v3.0/OS-AGENCY/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnDomain	-
DELETE /v3.0/OS-AGENCY/projects/{project_id}/agencies/{agency_id}/roles/{role_id}	iam:agencies:revokeRoleOnProject	-
GET /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/inherited_to_projects	iam:agencies:listRoles	-
PUT /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:grantRole	-

API	Action	Dependencies
HEAD /v3.0/OS-INHERIT/domains/{domain_id}/agencies/{agency_id}/roles/{role_id}/inherited_to_projects	iam:agencies:checkRole	-
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	-

API	Action	Dependencies
GET /v3.0/OS-PERMISSION/enterprise-projects/{enterprise_project_id}/users	iam::listUsersAssignedEnterpriseProject	-
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	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-217**, 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 IAM.

Table 5-217 Resource types supported by IAM

Resource Type	URN
policy	iam::<account-id>:policy:<policy-name-with-path>
agency	iam::<account-id>:agency:<agency-name-with-path>
user	iam::<account-id>:user:<user-name>
group	iam::<account-id>:group:<group-name>
mfa	iam::<account-id>:mfa:<mfa-name>

Conditions

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, 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, **iam:**) only apply to operations of the IAM service. For details, see **Table 5-218**.
  - 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.

The following table lists the condition keys that you can define in SCPs for IAM. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-218 Service-specific condition keys supported by IAM

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
iam:PolicyURN	string	Single-valued	Filters access by the URN of the identity policy
iam:ServicePrincipal	string	Single-valued	Filters access by the service ID of the cloud service transferred by the service-linked agency

5.10.13.4 Security Token Service (STS)

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 edit 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 Security Token Service (STS), 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 STS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for STS.

Table 5-219 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 *	g:ResourceTag/<tag-key>	-
			-	• **sts:ExternalId** • **sts:SourceIdentity** • **sts:TransitiveTagKeys** • **sts:AgencySessionName** • g:RequestTag/<tag-key> • g:TagKeys • g:SourceAccount • g:SourceUrn	

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
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 an STS session.	Write	agency *	g:ResourceTag/<tag-key>	-
			-	**sts:SourceIdentity**	
sts::tagSession	Grants permission to add tags to an STS session.	Tagging	agency *	g:ResourceTag/<tag-key>	-
			-	• **sts:TransitiveTagKeys** • g:RequestTag/<tag-key> • g:TagKeys	
sts::getServiceBearerToken	Grants permission to obtain a service bearer token.	Write	-	• **sts:DurationTimes** • **sts:ServiceName**	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-220**, 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 STS.

Table 5-220 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

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:) only apply to operations of the STS service. For details, see **Table 5-221**.
  - 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 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 5-221 Service-specific condition keys supported by STS

Service-specific Condition Key	Type	Single-valued/ 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:DurationTimes	numeric	Single-valued	Filters access by the duration time when you create a bearer token.
sts:ServiceName	string	Single-valued	Filters access by the service name when you create a bearer token.

5.10.13.5 Resource Formation Service (RFS)

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 Resource Formation Service (RFS), 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 Resource Formation Service (RFS), see **Conditions**.

The following table lists the actions that you can define in SCP statements for Resource Formation Service (RFS).

Table 5-222 Actions supported by Resource Formation Service (RFS)

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rf:privateTemplate:list	Grants permission to obtain private template list of project.	list	privateTemplate *	-
rf:privateTemplate:create	Grants permission to create a private template.	write	privateTemplate *	-
rf:privateTemplate:delete	Grants permission to delete a private template.	write	privateTemplate *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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 *	-
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 *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rf:stack:create	Grants permission to create a stack.	write	stack *	-
rf:stack:deploy	Grants permission to deploy a stack.	write	stack *	-
rf:stack:list	Grants permission to list all stacks.	list	stack *	-
rf:stack:getMetadata	Grants permission to get the metadata of a stack.	read	stack *	-
rf:stack:delete	Grants permission to delete a stack.	write	stack *	-
rf:stack:getTemplate	Grants permission to get the template of a stack.	read	stack *	-
rf:stack:listEvents	Grants permission to list deployment events of a stack.	list	stack *	-
rf:stack:listResources	Grants permission to list all resources of a stack.	list	stack *	-
rf:stack:listOutputs	Grants permission to list all outputs of a stack.	list	stack *	-
rf:stack:createExecutionPlan	Grants permission to create an execution plan.	write	stack *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
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 *	-
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:continueDeploy	Grants permission to continue to deploy the stack.	write	stack *	-
rf:stack:estimateExecutionPlanPrice	Grants permission to estimate the price of an execution plan.	read	stack *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rf:stack:update	Grants permission to update stack properties.	write	stack *	-
rf:stackSet:create	Grants permission to create a stack set.	write	stackSet *	-
rf:stackSet:list	Grants permission to list all stack sets.	list	stackSet *	-
rf:stackSet:showTemplate	Grants permission to show the template of a stack set.	read	stackSet *	-
rf:stackSet:showMetadata	Grants permission to show the metadata of a stack set.	read	stackSet *	-
rf:stackSet:deploy	Grants permission to deploy a stack set.	write	stackSet *	-
rf:stackSet:delete	Grants permission to delete a stack set.	write	stackSet *	-
rf:stackSet:update	Grants permission to update stack set properties.	write	stackSet *	-
rf:stackSet:listStackInstances	Grants permission to list all stack instances.	list	stackSet *	-
rf:stackSet:createStackInstances	Grants permission to create stack instances.	write	stackSet *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
rf:stackSet:deleteStackInstances	Grants permission to delete stack instances.	write	stackSet *	-
rf:stackSet:showOperationMetadata	Grants permission to show the metadata of an stack set operation.	read	stackSet *	-
rf:stackSet:listOperations	Grants permission to list all stack set operations.	list	stackSet *	-

Each API of Resource Formation Service (RFS) usually supports one or more actions. **Table 5-223** lists the supported actions and dependencies.

Table 5-223 Actions and dependencies supported by Resource Formation Service (RFS) 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	-

API	Action	Dependencies
POST /v1/{project_id}/templates/{template_name}/versions	rf:privateTemplate:createVersion	-
GET /v1/{project_id}/templates/{template_name}/versions/{version_id}	rf:privateTemplate:showVersionContent	-
DELETE /v1/{project_id}/templates/{template_name}/versions/{version_id}	rf:privateTemplate:deleteVersion	-
GET /v1/{project_id}/templates/{template_name}/versions/{version_id}/metadata	rf:privateTemplate:showVersionMetadata	-
POST /v1/{project_id}/stacks	rf:stack:create	• kms:cmk:decryptDataKey • iam:agencies:pass
POST /v1/{project_id}/stacks/{stack_name}/deployments	rf:stack:deploy	kms:cmk:decryptDataKey
GET /v1/{project_id}/stacks	rf:stack:list	-
GET /v1/{project_id}/stacks/{stack_name}/metadata	rf:stack:getMetadata	-
DELETE /v1/{project_id}/stacks/{stack_name}	rf:stack:delete	-
GET /v1/{project_id}/stacks/{stack_name}/templates	rf:stack:getTemplate	-
GET /v1/{project_id}/stacks/{stack_name}/events	rf:stack:listEvents	-
GET /v1/{project_id}/stacks/{stack_name}/resources	rf:stack:listResources	-
GET /v1/{project_id}/stacks/{stack_name}/outputs	rf:stack:listOutputs	-

API	Action	Dependencies
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:getExecutionPlanMetadata	-
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	-
GET /v1/{project_id}/stacks/{stack_name}/execution-plans/{execution_plan_name}/prices	rf:stack:estimateExecutionPlanPrice	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	-

API	Action	Dependencies
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 SCP applies to. If you specify a resource type for any action in **Table 5-224**, 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 Resource Formation Service (RFS).

Table 5-224 Resource types supported by Resource Formation Service (RFS)

Resource Typehttps://support.huaweicloud.com/usermanual-organizations/org_03_0033.html#section2	URN
privateTemplate	rf:<region>:<account-id>:privateTemplate:<template-name>

Resource Typehttps://support.huaweicloud.com/usermanual-organizations/org_03_0033.html#section2	URN
stackSet	rf:<region>:<account-id>:stackSet:<stack-set-name>/<stack-set-id>
stack	rf:<region>:<account-id>:stack:<stack-name>

Conditions

Resource Formation Service (RFS) 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.

5.10.13.6 IAM Identity Center

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** column indicates whether the action supports resource-level permissions.
  - You can use a wildcard (*) to indicate all resources. 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, 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 defined by IAM Identity Center, see **Resources**.

- The **Condition Key** column contains keys that you can specify in the Condition element of an SCP statement.
  - If the **Resource** column has values for an action, the condition key takes effect only for the listed resources.
  - If the **Resource** 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 Identity Center, see **Conditions**.

The following table lists the actions that you can define in SCP statements for IAM Identity Center.

Table 5-225 Actions supported by IAM Identity Center

Action	Description	Access Level	Resource (*: required)	Condition Key
IdentityCenter:permissionSet:create	Grants permission to create a permission set.	write	instance *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys
IdentityCenter:permissionSet:attachManagedPolicy	Grants permission to attach system-defined identity policies to a permission set.	permission_management	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:detachManagedPolicy	Grants permission to detach system-defined identity policies from a specified permission set.	permission_management	instance *	-
			permissionSet *	-

Action	Description	Access Level	Resource (*: required)	Condition Key
IdentityCenter:permissionSet:update	Grants permission to update the permission set of a specified instance.	permission_management	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:delete	Grants permission to delete the permission set of a specified instance.	write	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:list	Grants permission to list the permission sets of a specified instance.	list	instance *	-
IdentityCenter:permissionSet:listAccountsForProvisioned	Grants permission to list all the accounts provisioned by a specified permission set.	list	permissionSet *	-
			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 identity policies attached to a specified permission set.	list	instance *	-
			permissionSet *	-

Action	Description	Access Level	Resource (*: required)	Condition Key
IdentityCenter:permissionSet:listProvisionedToAccount	Grants permission to list all permission sets associated with a specified account.	list	account *	-
			instance *	-
IdentityCenter:permissionSet:describeProvisioning-Status	Grants permission to obtain the details of the permission set attachment status.	read	instance *	-
IdentityCenter:permissionSet:describe	Grants permission to obtain the permission set details of a specified instance.	read	instance *	-
			permissionSet *	-
IdentityCenter:permissionSet:provision	Grants permission to attach a specified permission set to a specified principal.	write	account *	-
			instance *	-
			permissionSet *	-
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	-	-

Action	Description	Access Level	Resource (*: required)	Condition Key
IdentityCenter:instance:deleteIdentityCenter	Grants permission to disable IAM Identity Center.	write	-	-
IdentityCenter:instance:list	Grants permission to query the IAM Identity Center instance list.	list	-	-
IdentityCenter:accountAssignment:create	Grants permission to assign access to principals for a specified account using a specified permission set.	write	instance *	-
			account *	-
			permissionSet *	-
IdentityCenter:accountAssignment:delete	Grants permission to delete a principal's access from a specified account using a specified permission set.	write	instance *	-
			account *	-
			permissionSet *	-
IdentityCenter:accountAssignment:list	Grants permission to list the assignee of the specified account with the specified permission set.	list	instance *	-
			account *	-
			permissionSet *	-
IdentityCenter:accountAssignment:describeDeletionStatus	Grants permission to obtain the details about the status of the assignment deletion request.	read	instance *	-

Action	Description	Access Level	Resource (*: required)	Condition Key
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 *	-
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:listProfileAssociation	Grants permission to query all users or groups associated with an account or permission set.	read	-	-
IdentityCenter:accountAssignment:disassociationProfile	Grants permission to disassociate all authorizations from a user or group.	write	-	-

Action	Description	Access Level	Resource (*: required)	Condition Key
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	-	-
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:user:create	Grants permission to create a user.	write	-	-
IdentityCenter:user:list	Grants permission to query the user list.	read	-	-

Action	Description	Access Level	Resource (*: required)	Condition Key
IdentityCenter:user:describe	Grants permission to query user details.	read	-	-
IdentityCenter:user:describeUsers	Grants permission to obtain user details in batch.	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	-	-
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 obtain group details in batch.	read	-	-

Action	Description	Access Level	Resource (*: required)	Condition Key
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	-	-
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	-	-

Action	Description	Access Level	Resource (*: required)	Condition Key
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	-	-
IdentityCenter:externalIdp:enable	Grants permission to enable an external identity provider.	write	-	-
IdentityCenter:externalIdp:disable	Grants permission to disable an external identity provider.	write	-	-
IdentityCenter:externalIdp:getSpConfiguration	Grants permission to obtain the configuration of the IAM Identity Center service provider.	read	-	-
IdentityCenter:externalIdp:update	Grants permission to update the configuration of the external identity provider.	write	-	-
IdentityCenter:externalIdp:delete	Grants permission to delete the configuration of the external identity provider.	write	-	-

Action	Description	Access Level	Resource (*: required)	Condition Key
IdentityCenter:externalIdp:importCertificate	Grants permission to import a certificate.	write	-	-
IdentityCenter:externalIdp:deleteCertificate	Grants permission to delete a certificate.	write	-	-
IdentityCenter:externalIdp:listCertificates	Grants permission to obtain the certificate list.	read	-	-
IdentityCenter:externalIdp:createProvisioningTenant	Grants permission to create a tenant.	write	-	-
IdentityCenter:externalIdp:listProvisioningTenant	Grants permission to query the tenant list.	read	-	-
IdentityCenter:externalIdp:deleteProvisioningTenant	Grants permission to delete a tenant.	write	-	-
IdentityCenter:externalIdp:createBearerToken	Grants permission to create a bearer token.	write	-	-
IdentityCenter:externalIdp:listBearerTokens	Grants permission to query the bearer token list.	read	-	-
IdentityCenter:externalIdp:deleteBearerToken	Grants permission to delete a bearer token.	write	-	-

Action	Description	Access Level	Resource (*: required)	Condition Key
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	-	-

Each API of IAM Identity Center usually supports one or more actions. **Table 5-226** lists the supported actions and dependencies.

Table 5-226 Actions and dependencies supported by IAM Identity Center APIs

API	Action	Dependencies
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	• iam:policies:get • organizations:delegatedAdministrators:list
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
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

API	Action	Dependencies
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/instances	IdentityCenter:instance:list	organizations:delegatedAdministrators:list
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/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

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}/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
PUT /v1/identity-stores/{identity_store_id}/groups/{group_id}	IdentityCenter:group:update	organizations:delegatedAdministrators:list
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:groupMemberships:list	organizations:delegatedAdministrators:list
GET /v1/identity-stores/{identity_store_id}/group-memberships-for-member	IdentityCenter:groupMembership:listForMember	organizations:delegatedAdministrators:list

API	Action	Dependencies
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
POST /v1/identity-stores/{identity_store_id}/is-member-in-groups	IdentityCenter:groupMembership:isMembershipInGroup	organizations:delegatedAdministrators:list

Resources

A resource is what a policy applies to. If you specify a resource for any action in **Table 5-227**, the resource URN must be specified in the policy statements using that action, and the policy applies only to these resources. If no resources are 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 resources.

The following table lists the resources that you can define in SCP statements for IAM Identity Center.

Table 5-227 Resources supported by IAM Identity Center

Resource	URN
instance	IdentityCenter::<management-account-id>:instance:<instance-id>
account	IdentityCenter::<management-account-id>:account:<account-id>
permissionSet	IdentityCenter::<management-account-id>:permissionSet:<instance-id>/<permission-set-id>

Conditions

IAM Identity Center 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.

5.10.13.7 Organizations

The Organizations service provides Service Control Policies 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 (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 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 Organizations, 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 of an action is empty (-), the action does not support any condition keys.

  For details about the condition keys defined by Organizations, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Organizations.

Table 5-228 Actions supported by Organizations

Action	Description	Access Level	Resource Type (*: required)	Condition Key
organizations:organizations:create	Grants permission to create an organization.	write	-	-
organizations:organizations:get	Grants permission to get organization information.	read	-	-
organizations:organizations:delete	Grants permission to delete an organization.	write	-	-
organizations:organizations:leave	Grants permission to leave the current organization.	write	-	-
organizations:roots:list	Grants permission to list the root of an organization.	list	-	-
organizations:ous:create	Grants permission to create an OU.	write	ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:ous:list	Grants permission to list OUs.	list	-	-
organizations:ous:get	Grants permission to get OU information.	read	ou *	g:ResourceTag/<tag-key>
organizations:ous:update	Grants permission to rename an OU.	write	ou *	g:ResourceTag/<tag-key>
organizations:ous:delete	Grants permission to delete an OU.	write	ou *	g:ResourceTag/<tag-key>
organizations:accounts:create	Grants permission to create an account.	write	-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
organizations:accounts:list	Grants permission to list accounts in an organization.	list	-	-
organizations:accounts:get	Grants permission to get account information.	read	account *	g:ResourceTag/<tag-key>
organizations:accounts:remove	Grants permission to remove the specified account.	write	account *	g:ResourceTag/<tag-key>
organizations:accounts:move	Grants permission to move an account.	write	account *	g:ResourceTag/<tag-key>
organizations:accounts:invite	Grants permission to invite an account to join an organization.	write	-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:createAccountStatuses:list	Grants permission to list the account creation status.	list	-	-
organizations:createAccountStatuses:get	Grants permission to get information about the account creation status.	read	-	-
organizations:handshakes:get	Grants permission to get invitation information.	read	handshake *	-
organizations:handshakes:accept	Grants permission to accept an invitation.	write	handshake *	-
organizations:handshakes:decline	Grants permission to reject an invitation.	write	handshake *	-
organizations:handshakes:cancel	Grants permission to cancel an invitation.	write	handshake *	-
organizations:receivedHandshakes:list	Grants permission to list received invitations.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
organizations:handshakes:list	Grants permission to list sent invitations.	list	-	-
organizations:trustedServices:enable	Grants permission to enable a trusted service.	write	-	organizations:ServicePrincipal
organizations:trustedServices:disable	Grants permission to disable a trusted service.	write	-	organizations:ServicePrincipal
organizations:trustedServices:list	Grants permission to list trusted services.	list	-	-
organizations:delegatedAdministrators:register	Grants permission to register a delegated administrator.	write	account *	g:ResourceTag/<tag-key>
			-	organizations:ServicePrincipal
organizations:delegatedAdministrators:deregister	Grants permission to deregister a delegated administrator.	write	account *	g:ResourceTag/<tag-key>
			-	organizations:ServicePrincipal
organizations:delegatedServices:list	Grants permission to list services managed by a delegated administrator account.	list	account *	g:ResourceTag/<tag-key>
organizations:delegatedAdministrators:list	Grants permission to list delegated administrator accounts.	list	-	organizations:ServicePrincipal
organizations:policies:create	Grants permission to create a policy.	write	-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:policies:list	Grants permission to list policies.	list	-	-
organizations:policies:get	Grants permission to get policy information.	read	policy *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
organizations:policies:update	Grants permission to update a policy.	write	policy *	g:ResourceTag/<tag-key>
organizations:policies:delete	Grants permission to delete a policy.	write	policy *	g:ResourceTag/<tag-key>
organizations:policies:enable	Grants permission to enable a policy type for a root.	write	root *	g:ResourceTag/<tag-key>
organizations:policies:disable	Grants permission to disable a policy type for a root.	write	root *	g:ResourceTag/<tag-key>
organizations:policies:attach	Grants permission to attach a policy to a principal.	write	policy *	g:ResourceTag/<tag-key>
			account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
organizations:policies:detach	Grants permission to detach a policy from a principal.	write	policy *	g:ResourceTag/<tag-key>
			account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
organizations:attachedEntities:list	Grants permission to list entities for the specified policy.	list	policy *	g:ResourceTag/<tag-key>
organizations:tags:list	Grants permission to list tags attached to the specified resource.	list	account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
			policy	g:ResourceTag/<tag-key>
organizations:resources:tag	Grants permission to tag the specified resource.	tagging	account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
			policy	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:resources:untag	Grants permission to untag the specified resource.	tagging	account	g:ResourceTag/<tag-key>
			ou	g:ResourceTag/<tag-key>
			root	g:ResourceTag/<tag-key>
			policy	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
organizations:entities:list	Grants permission to list entities in an organization.	list	-	-
organizations:services:list	Grants permission to list cloud services integrable with Organizations.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
organizations:tagPolicyServices:list	Grants permission to list the resource types that support tag policy enforcement.	list	-	-
organizations:effectivePolicies:get	Grants permission to get the effective policy of a specified type.	read	-	-
organizations:resources:listByTag	Grants permission to list instances by resource type and tag.	list	-	-
organizations:resources:countByTag	Grants permission to list the number of instances by resource type and tag.	list	-	-
organizations:resources:list	Grants permission to list project tags.	list	-	-
organizations:quotas:list	Grants permission to list organization quotas.	list	-	-

Each API of Organizations usually supports one or more actions. **Table 5-229** lists the supported actions and dependencies.

Table 5-229 Actions and dependencies supported by Organizations APIs

API	Action	Dependencies
POST /v1/organizations	organizations:organizations:create	iam:agencies:createServiceLinkedAgency
GET /v1/organizations	organizations:organizations:get	-
DELETE /v1/organizations	organizations:organizations:delete	-

API	Action	Dependencies
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	-
PATCH /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:update	-
DELETE /v1/organizations/organizational-units/{organizational_unit_id}	organizations:ous:delete	-
POST /v1/organizations/accounts	organizations:accounts:create	organizations:resources:tag
GET /v1/organizations/accounts	organizations:accounts:list	-
GET /v1/organizations/accounts/{account_id}	organizations:accounts:get	-
POST /v1/organizations/accounts/{account_id}/remove	organizations:accounts:remove	-

API	Action	Dependencies
POST /v1/organizations/accounts/{account_id}/move	organizations:accounts:move	-
POST /v1/organizations/accounts/invite	organizations:accounts:invite	organizations:resources:tag
GET /v1/organizations/create-account-status	organizations:createAccountStatuses: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:createServiceLinkedAgency
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	-

API	Action	Dependencies
POST /v1/organizations/trusted-services/disable	organizations:trustedServices:disable	-
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	-

API	Action	Dependencies
POST /v1/organizations/policies/enable	organizations:policies:enable	-
POST /v1/organizations/policies/disable	organizations:policies:disable	-
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	-

API	Action	Dependencies
GET /v1/organizations/{resource_type}/{resource_id}/tags	organizations:tags:list	-
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 SCP applies to. If you specify a resource type for any action in **Table 5-230**, 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 Organizations.

Table 5-230 Resource types supported by Organizations

Resource Type	URN
handshake	organizations::<management-account-id>:handshake:<organization-id>/<handshake-id>
ou	organizations::<management-account-id>:ou:<organization-id>/<organization-unit-id>
organization	organizations::<management-account-id>:organization:<organization-id>
root	organizations::<management-account-id>:root:<organization-id>/<root-id>
account	organizations::<management-account-id>:account:<organization-id>/<account-id>
policy	organizations::<management-account-id>:policy:<organization-id>/<policy-type>/<policy-id>
builtinpolicy	organizations::system:policy:<policy-type>/<policy-id>

Conditions

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, **organizations:**) only apply to operations of the Organizations service. For details, see **Table 5-231**.
  - 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.

The following table lists the condition keys that you can define in SCPs for Organizations. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-231 Service-specific condition keys supported by Organizations

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
organizations:ServicePrincipal	string	Single-valued	Filters access based on the name of the specified service principal

5.10.13.8 Resource Access Manager (RAM)

The Organizations service provides Service Control Policies 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.

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 RAM, 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 RAM, see **Conditions**.

The following table lists the actions that you can define in SCP statements for RAM.

Table 5-232 Actions supported by RAM

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ram:permissions:list	Grants permission to list RAM permissions.	list	permission *	-
ram:permissions:get	Grants permission to get the details of an RAM permission.	read	permission *	-
ram:resourceShares:create	Grants permission to create a resource share with provided resources and/or principals.	write	-	• g:RequestTag/<tag-key> • g:TagKeys • ram:RequestedResourceType • ram:ResourceUrn • ram:Principal • ram:TargetOrgPaths • ram:RequestedAllowExternalPrincipals
ram:resourceShares:search	Grants permission to search for a set of resource shares from a provided list or with a specified state.	read	-	• g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ram:resourceShares:update	Grants permission to update the attributes of a resource share.	write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals
			-	ram:RequestedAllowExternalPrincipals
ram:resourceShares:delete	Grants permission to delete a resource share.	write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals
ram:resourceShares:associate	Grants permission to associate resources and/or principals to a resource share.	write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals
			-	• ram:RequestedResourceType • ram:ResourceUrn • ram:Principal • ram:TargetOrgPaths
ram:resourceShares:disassociate	Grants permission to disassociate resources and/or principals from a resource share.	write	resourceShare *	• g:ResourceTag/<tag-key> • ram:AllowExternalPrincipals
			-	• ram:RequestedResourceType • ram:ResourceUrn • ram:Principal • ram:TargetOrgPaths

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ram:resourceShares:searchResourceShareAssociations	Grants permission to search for a set of resource share associations from a provided list or with a specified state of the specified type.	read	-	-
ram:resourceShares:associatePermission	Grants permission to associate a permission with a resource share.	write	resourceShare*	g:ResourceTag/<tag-key>
			-	ram:PermissionUrn
ram:resourceShares:disassociatePermission	Grants permission to disassociate a permission from a resource share.	write	resourceShare*	g:ResourceTag/<tag-key>
			-	ram:PermissionUrn
ram:resourceShares:listAssociatedPermissions	Grants permission to list the permissions associated with a resource share.	list	resourceShare*	g:ResourceTag/<tag-key>
ram:resourceShares:tag	Grants permission to tag the specified resource share.	tagging	resourceShare*	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
ram:resourceShares:untag	Grants permission to untag the specified resource share.	tagging	resourceShare*	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
ram:resourceShares:listTags	Grants permission to list tags attached to a resource share.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ram:resourceShares:listResourceSharesByTag	Grants permission to list resource shares by tag.	list	-	• g:TagKeys
ram:resourceShares:searchResourceShareCountByTag	Grants permission to search for the number of resource shares by tag.	read	-	• g:TagKeys
ram:sharedResources:search	Grants permission to search for the resources that you added to a resource share or that are shared with you.	list	-	-
ram:sharedPrincipals:search	Grants permission to search for 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 sharing invitation.	write	resourceShareInvitation *	-
			-	ram:ShareOwnerAccountId
ram:resourceShareInvitations:reject	Grants permission to reject the specified resource sharing invitation.	write	resourceShareInvitation *	-
			-	ram:ShareOwnerAccountId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ram:resourceShareInvitations:search	Grants permission to search for resource sharing invitations by the specified invitation ID or resource share ID.	read	-	-
ram:resourceShares:enableSharingWithOrganization	Grants permission to enable sharing with Organizations.	permission_management	-	-
ram:resourceShares:disableSharingWithOrganization	Grants permission to disable sharing with Organizations.	permission_management	-	-
ram:resourceShares:searchEnableSharingWithOrganization	Grants permission to check whether sharing with Organizations is enabled.	read	-	-
ram:sharedResources:searchDistinctResource	Grants permission to search for the distinct resources that you added to a resource share or that are shared with you.	list	-	-
ram:sharedPrincipals:searchDistinctPrincipal	Grants permission to search for the distinct principals that you have shared resources with or that have shared resources with you.	list	-	-
ram:resourceShares:listQuota	Grants permission to list the quotas of resource sharing.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ram:resourceTypes:list	Grants permission to list the resource types of cloud services.	list	-	-
ram:permission:listVersions	Grants permission to list all versions of the specified RAM permission.	list	-	-

Each API of RAM usually supports one or more actions. #org_20_0042/en-us_topic_0000001865665109_en-us_topic_0000001679340620_api_relation_table lists the supported actions and dependencies.

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-233**, 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 RAM.

Table 5-233 Resource types supported by RAM

Resource Type	URN
permission	ram::system:permission:<permission-id>
resourceShare	ram::<account-id>:resourceShare:<resource-share-id>
resourceShareInvitation	ram::<account-id>:resourceShareInvitation:<resource-share-invitation-id>

Conditions

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 as the prefix, for example, **ram:**) apply only to operations of the RAM service. For details, see **Table 5-234**.
  - 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 SCP 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 RAM. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-234 Service-specific condition keys supported by RAM

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
ram:RequestedResourceType	string	Multivalued	Filters access by the specified resource type.
ram:ResourceUrn	string	Multivalued	Filters access by resources with the specified URN.
ram:Principal	string	Multivalued	Filters access by the format of the specified principal.
ram:TargetOrgPaths	string	Multivalued	Filters access by the organization path of the specified principal.
ram:PermissionUrn	string	Single-valued	Filters access by the specified permission URN.

Service-specific Condition Key	Type	Single-valued/ Multivalued	Description
ram:ShareOwnerAccountId	string	Single-valued	Filters access by resource shares owned by a specific account. For example, you can use this condition key to specify which resource sharing invitations can be accepted or rejected based on the resource 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 the value **true** if you only allow the action for resource shares that can be associated with external principals. External principals refer to accounts outside your organization.
ram:RequestedAllowExternalPrincipals	boolean	Single-valued	Filters access by the specified value for **allow_external_principals**. External principals refer to accounts outside your organization.

5.10.13.9 Enterprise Project Management Service (EPS)

Organizations provides your with Service Control Policies 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 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.

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** 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 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 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 this column is empty (-), the action does not support any condition keys.

  For details about the condition keys defined by EPS, see **Conditions**.

The following table lists the actions that you can define in custom policies for EPS.

Table 5-235 Supported Actions

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
eps:enterpriseProjects:list	Grants permission to list enterprise projects.	list	enterpriseProject *	-
eps:enterpriseProjects:create	Grants permission to create enterprise projects.	write	enterpriseProject *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
eps:enterpriseProjects:update	Grants permission to modify enterprise projects.	write	enterpriseProject *	-
eps:enterpriseProjects:enable	Grants permission to enable enterprise projects.	write	enterpriseProject *	-
eps:enterpriseProjects:disable	Grants permission to disable enterprise projects.	write	enterpriseProject *	-
eps:resources:list	Grants permission to list resources in an enterprise project.	list	enterpriseProject *	-
eps:resources:add	Grants permission to add resources to an enterprise project.	write	enterpriseProject *	-
eps:resources:remove	Grants permission to remove resources from an enterprise project.	write	enterpriseProject *	-

An EPS API usually supports one or more actions. **Table 5-236** lists actions supported by each API and dependencies of actions.

Table 5-236 APIs and actions

API	Action	Dependencies
GET /v1.0/enterprise-projects	eps:enterpriseProjects:list	-

API	Action	Dependencies
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	-
POST /v1.0/enterprise-projects/{enterprise_project_id}/action	eps:enterpriseProjects:disable	-
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
POST /v1.0/enterprise-projects/{enterprise_project_id}/resources-migrate	eps:resources:remove	eps:resources:add

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-237**, 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 EPS.

Table 5-237 Resources supported by EPS

Resource Type	URN
enterpriseProject	eps::<account-id>:enterpriseProject:<enterprise-project-id>

Conditions

EPS does not support service-specific condition keys in an SCP.

You can only use global condition keys. Global condition keys are applicable to all services. For details, see Condition Keys.

5.10.13.10 Tag Management Service (TMS)

Organizations provides your with Service Control Policies 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 only 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 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 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 this column is empty (-), the action does not support any condition keys.

For details about the condition keys defined by TMS, see **Conditions**.

The following table lists the actions that you can define in custom policies for TMS.

Table 5-238 Supported actions

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
tms:predefineTags:list	Grants permission to query predefined tags.	list	-	-
tms:predefineTags:create	Grants permission to create predefined tags.	write	-	-
tms:predefineTags:update	Grants permission to modify predefined tags.	write	-	-
tms:predefineTags:delete	Grants permission to delete predefined tags.	write	-	-
tms:resourceTags:list	Grants permission to list resource tags.	list	-	-
tms:resourceTags:create	Grants permission to create resource tags.	write	-	-
tms:resourceTags:delete	Grants permission to delete resource tags.	write	-	-
tms:resources:list	Grants permission to list resources.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
tms:tagKeys:list	Grants permission to list tag keys.	list	-	-
tms:tagValues:list	Grants permission to list tag values.	list	-	-

A TMS API usually supports one or more actions. **Table 5-239** lists actions supported by each API and dependencies of actions.

Table 5-239 APIs and actions

API	Action	Dependencies
GET /v1.0/predefine_tags	tms:predefineTags:list	-
POST /v1.0/predefine_tags/action	tms:predefineTags:create	-
PUT /v1.0/predefine_tags	tms:predefineTags:update	-
POST /v1.0/predefine_tags/action	tms:predefineTags:delete	-
GET /v2.0/resources/{resource_id}/tags	tms:resourceTags:list	-
POST /v1.0/resource-tags/batch-create	tms:resourceTags:create	-
POST /v1.0/resource-tags/batch-delete	tms:resourceTags:delete	-
POST /v1.0/resource-instances/filter	tms:resources:list	-
GET /v1.0/tag-keys	tms:tagKeys:list	-
GET /v1.0/tag-values	tms:tagValues:list	-

Resources

TMS does not support granting permissions for specific resources using SCPs To allow access to TMS, use the wildcard (*) in the Resource element in an SCP, and this SCP will apply to all resources of TMS.

Conditions

TMS does not support service-specific condition keys in an SCP.

You can only use global condition keys. Condition keys are applicable to all services. For details, see Condition Keys.

5.10.13.11 Config

Organizations provides your with Service Control Policies 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 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 in 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 resource 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 Config, 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 this column is empty (-), the action does not support any condition keys.

  For details about the condition keys defined by Config, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Config.

Table 5-240 Actions supported by Config

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
rms:organizationConformancePacks:create	Grants permission to create organization conformance packages.	write	-	-
rms:organizationConformancePacks:get	Grants permission to view organization conformance packages.	read	organizationConformancePacks *	-
rms:organizationConformancePacks:delete	Grants permission to delete organization conformance packages.	write	organizationConformancePacks *	-
rms:organizationConformancePacks:update	Grants permission to update organization conformance packages.	write	organizationConformancePacks *	-
rms:organizationConformancePacks:list	Grants permission to list organization conformance packages.	list	-	-
rms:conformancePacks:create	Grants permission to create conformance packages.	write	-	-
rms:conformancePacks:get	Grants permission to view conformance packages.	read	conformancePacks *	-
rms:conformancePacks:delete	Grants permission to delete conformance packages.	write	conformancePacks *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
rms:conformancePacks:update	Grants permission to update conformance packages.	write	conformancePacks *	-
rms:conformancePacks:list	Grants permission to list conformance packages.	list	-	-
rms:storedQueries:create	Grants permission to save new advanced queries.	write	-	-
rms:storedQueries:update	Grants permission to modify advanced queries.	write	storedQueries *	-
rms:storedQueries:delete	Grants permission to delete advanced query statements.	write	storedQueries *	-
rms:storedQueries:get	Grants permission to view advanced query details.	read	storedQueries *	-
rms:storedQueries:list	Grants permission to list advanced queries.	list	-	-
rms:policyAssignments:create	Grants permission to create rules.	write	-	• g:TagKeys • g:RequestTag/<tag-key>
rms:policyAssignments:update	Grants permission to update rules.	write	policyAssignments *	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
rms:policyAssignments:delete	Grants permission to delete rules and their evaluation results.	write	policyAssignments *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
rms:policyAssignments:get	Grants permission to view rule details.	read	policyAssignments *	g:ResourceTag/<tag-key>
rms:organizationPolicyAssignments:put	Grants permission to create or update organization rules.	write	-	-
rms:organizationPolicyAssignments:delete	Grants permission to delete specific organization rules and their evaluation results.	write	organizationPolicyAssignments *	-
rms:organizationPolicyAssignments:get	Grants permission to view organization rule details.	read	organizationPolicyAssignments *	-
rms:organizationPolicyAssignments:list	Grants permission to list organization rules.	list	-	-
rms:policyStates:get	Grants permission to list rule evaluation results.	read	policyAssignments	g:ResourceTag/<tag-key>
rms:policyStates:runEvaluation	Grants permission to run specific rules.	write	policyAssignments	g:ResourceTag/<tag-key>
rms:policyStates:update	Grants permission to deliver evaluation results from FunctionGraph Config.	write	-	-
rms:aggregators:create	Grants permission to create aggregators.	write	-	-
rms:aggregators:update	Grants permission to update aggregators.	write	aggregators *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
rms:aggregators:delete	Grants permission to delete specific aggregators.	write	aggregators *	-
rms:aggregators:list	Grants permission to list aggregators.	list	-	-
rms:aggregators:get	Grants permission to view aggregator details.	read	aggregators *	-
rms:aggregatorResources:list	Grants permission to view aggregated resources.	list	-	-
rms:aggregatorResources:runQuery	Grants permission to run advanced queries for querying attributes of aggregated resources.	list	-	-
rms:aggregatorResources:get	Grants permission to view details of aggregated resources	read	-	-
rms:aggregationAuthorizations:create	Grants permission to create aggregation authorization.	write	aggregationAuthorizations *	-
			-	rms:AuthorizedAccountOrgPath
rms:aggregationAuthorizations:list	Grants permission to list aggregator authorization.	list	-	-
rms:aggregationAuthorizations:delete	Grants permission to revoke aggregation authorization.	write	aggregationAuthorizations *	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
			-	rms:AuthorizedAccountOrgPath
rms:aggregationRequests:delete	Grants permission to delete aggregation requests from other accounts.	write	-	-
rms:aggregationRequests:list	Grants permission to list aggregation requests from other accounts.	list	-	-
rms:trackerConfig:put	Grants permission to enable the resource recorder or modify resource recorder configurations.	write	-	• rms:TrackerBucketName • rms:TrackerBucketPathPrefix
rms:trackerConfig:delete	Grants permission to disable the resource recorder.	write	-	-
rms:trackerConfig:get	Grants permission to view resource recorder configurations.	read	-	-
rms:schemas:list	Grants permission to view schemas of advanced queries.	list	-	-
rms:policyDefinitions:get	Grants permission to view built-in policies.	list	-	-
rms:resources:getHistory	Grants permission to view resource configuration history.	list	-	-
rms:resources:getRelation	Grants permission to view resource relationships.	list	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
rms:resources:get	Grants permission to view details of specific resources.	read	-	-
rms:resources:list	Grants permission to list resources.	list	-	-
rms:resources:runQuery	Grants permission to run advanced queries.	list	-	-
rms:resources:summarize	Grants permission to view resource overview.	list	-	-
rms::tagResource	Grants permission to batch create resource tags.	tagging	policyAssignments	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
rms::unTagResource	Grants permission to batch delete resource tags.	tagging	policyAssignments	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
rms::listTagsForResource	Grants permission to query resource tags.	list	policyAssignments	g:ResourceTag/<tag-key>
rms::listTags	Grants permission to query project tags.	list	-	-
rms::listResourcesByTag	Grants permission to query resources by tag.	list	-	g:TagKeys
rms:policyAssignmentsRemediation:putRemediationConfiguration	Grants permission to add remediation configurations.	write	policyAssignmentsRemediation*	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
rms:policyAssignmentsRemediation:deleteRemediationConfiguration	Grants permission to delete remediation configurations.	write	policyAssignmentsRemediation *	-
rms:policyAssignmentsRemediation:getRemediationConfiguration	Grants permission to check remediation configurations.	read	policyAssignmentsRemediation *	-
rms:policyAssignmentsRemediation:runRemediation	Grants permission to run remediation execution.	write	policyAssignmentsRemediation *	-
rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	Grants permission to check remediation execution status.	list	policyAssignmentsRemediation *	-
rms:policyAssignmentsRemediation:createRemediationExceptions	Grants permission to create remediation exceptions.	write	policyAssignmentsRemediation *	-
rms:policyAssignmentsRemediation:deleteRemediationExceptions	Grants permission to delete remediation exceptions.	write	policyAssignmentsRemediation *	-
rms:policyAssignmentsRemediation:listRemediationExceptions	Grants permission to check remediation exceptions.	list	policyAssignmentsRemediation *	-

A Config API usually supports one or more actions. **Table 5-241** lists actions supported by each API and dependencies of actions.

Table 5-241 APIs and actions

API	Action	Dependencies
POST /v1/resource-manager/organizations/{organization_id}/conformance-packs	rms:organizationConformancePacks:create	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list
DELETE /v1/resource-manager/organizations/{organization_id}/conformance-packs/{conformance_pack_id}	rms:organizationConformancePacks:delete	organizations:organizations:get
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

API	Action	Dependencies
POST /v1/resource-manager/domains/{domain_id}/conformance-packs	rms:conformancePacks:create	• rf:stack:createStack • rf:stack:getStackMetadata • rf:stack:listStackResources
DELETE /v1/resource-manager/domains/{domain_id}/conformance-packs/{conformance_pack_id}	rms:conformancePacks:delete	• rf:stack:deleteStack • rf:stack:getStackMetadata
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	• organizations:organizations:get • organizations:accounts:list • organizations:delegatedAdministrators:list • organizations:trustedServices:enable • organizations:trustedServices:list
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	-
PUT /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:update	-
DELETE /v1/resource-manager/domains/{domain_id}/aggregators/{aggregator_id}	rms:aggregators:delete	-
GET /v1/resource-manager/domains/{domain_id}/aggregators	rms:aggregators:list	-
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	-

API	Action	Dependencies
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-summary	rms:aggregatorResources:list	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignments/compliance	rms:aggregatorResources:list	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-states/compliance-details	rms:aggregatorResources:list	-
POST /v1/resource-manager/domains/{domain_id}/aggregators/aggregate-data/policy-assignment/detail	rms:aggregatorResources:list	-
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	-

API	Action	Dependencies
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	-
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
GET /v1/resource-manager/domains/{domain_id}/tracked-resources	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/count	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/tags	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/summary	rms:resources:list	-
GET /v1/resource-manager/domains/{domain_id}/tracked-resources/{resource_id}	rms:resources:get	-
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	-

API	Action	Dependencies
POST /v1/resource-manager/{resource_type}/resource-instances/count	rms::listResourcesByTag	-
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	• iam:agencies:pass • iam:agencies:createServiceLinkedAgencyV5
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	• functiongraph:function:invokeAsync • functiongraph:function:getFunctionConfig • rf:stack:create • rf:stack:delete • rf:stack:getTemplate • rf:stack:getMetadata • rf:privateTemplate:showMetadata

API	Action	Dependencies
GET /v1/resource-manager/domains/{domain_id}/policy-assignments/{policy_assignment_id}/remediation-execution-statuses	rms:policyAssignmentsRemediation:listRemediationExecutionStatuses	-
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 SCP policy applies to. If you specify a resource type for any action in **Table 5-242**, 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 Config.

Table 5-242 Resources supported by Config

Resource Type	URN
conformancePacks	rms::<account-id>:conformancePacks:<conformance-pack-id>
storedQueries	rms::<account-id>:storedQueries:<query-id>
policyAssignments	rms::<account-id>:policyAssignments:<policy-assignment-id>
organizationPolicyAssignments	rms::<account-id>:organizationPolicyAssignments:<organization-id>/<organization-policy-assignments-id>
organizationConformancePacks	rms::<account-id>:organizationConformancePacks:<organization-id>/<organization-conformance-pack-id>
aggregators	rms::<account-id>:aggregators:<aggregator-id>
aggregationAuthorizations	rms::<account-id>:aggregationAuthorizations:<authorized-account-id>
policyAssignmentsRemediation	rms::<account-id>:policyAssignmentsRemediation:<policy-assignment-id>

Conditions

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

- A key in the Condition element of a 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.
  - A service-specific condition key is prefixed by the service name (such as **config:**) and applies only to a specific service. For details, see **Table 5-243**.
  - 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 constitute a complete condition statement. An SCP takes effect only when the statement meets related requirements. For supported condition operators, see SCP Syntax.

The following table lists the condition keys that you can define in SCPs for Config. You can include these condition keys to specify conditions for when your SCP is in effect.

Table 5-243 Service-level condition keys supported by Config

Service-Level Condition Key	Type	Single-valued/ Multi-valued	Description
rms:AuthorizedAccountOrg...	string	Single-valued	Access is controlled based on the **Organizations Path** of the specified aggregator account.
rms:TrackerBucketName	string	Single-valued	Access is controlled based on the specified bucket name.
rms:TrackerBucketPathPre...	string	Single-valued	Access is controlled based on the prefix of the specified OBS bucket.

Condition Key Examples

- rms:AuthorizedAccountOrgPath

  Preventing an organization member from giving aggregation authorization to accounts outside the organization

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:aggregationAuthorizations:create"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:AuthorizedAccountOrgPath": [
            "organization_id/root_id/ou_id" [Note: Enter the path ID of the organization.]
          ]
        }
      }
    }
  ]
}
```


- rms:TrackerBucketName

  Preventing the resource recorder from storing resource data to unexpected OBS buckets

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketName": [
            "BucketName"
          ]
        }
      }
    }
  ]
}
```

- rms:TrackerBucketPathPrefix

  Preventing storing resource data to unexpected OBS paths

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "rms:trackerConfig:put"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringNotMatch": {
          "rms:TrackerBucketPathPrefix": [
            "BucketFolder"
          ]
        }
      }
    }
  ]
}
```

5.10.13.12 IAM Access Analyzer

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 IAM Access Analyzer, 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 IAM Access Analyzer, see **Conditions**.

The following table lists the actions that you can define in SCP statements for IAM Access Analyzer.

Table 5-244 Actions supported by IAM Access Analyzer

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AccessAnalyzer:analyzer:create	Grants permission to create an access analyzer.	Write	analyzer *	-
			-	• g:RequestTag/<tag-key> • g:TagKeys

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AccessAnalyzer:analyzer:get	Grants permission to retrieve the access analyzer information.	Read	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:list	Grants permission to list access analyzers.	List	analyzer *	-
AccessAnalyzer:analyzer:delete	Grants permission to delete 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>
AccessAnalyzer:analyzer:listFindings	Grants permission to list findings.	List	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:updateFindings	Grants permission to update the findings.	Write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer::tagResource	Grants permission to add a tag to a resource.	Tagging	analyzer *	g:ResourceTag/<tag-key>
			-	• g:RequestTag/<tag-key> • g:TagKeys
AccessAnalyzer::untagResource	Grants permission to remove a tag from a resource.	Tagging	analyzer *	g:ResourceTag/<tag-key>
			-	g:TagKeys
AccessAnalyzer:archiveRule:create	Grants permission to create an archive rule for the specified access analyzer.	Write	archiveRule *	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AccessAnalyzer:archiveRule:get	Grants permission to retrieve an archive rule for the specified access analyzer.	Read	archiveRule *	-
AccessAnalyzer:archiveRule:list	Grants permission to list archive rules for the specified access analyzer.	List	archiveRule *	-
AccessAnalyzer:archiveRule:update	Grants permission to modify an archive rule for the specified access analyzer.	Write	archiveRule *	-
AccessAnalyzer:archiveRule:delete	Grants permission to delete an 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 *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:getPreview	Grants permission to retrieve an access preview for the specified access analyzer.	Read	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:listPreviews	Grants permission to list access previews for the specified access analyzer.	List	analyzer *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AccessAnalyzer:analyzer:listPreviewFindings	Grants permission to list access preview findings for the specified access analyzer.	List	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:createResourceConfigurations	Grants permission to create resource configurations.	Write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:listResourceConfigurations	Grants permission to list resource configurations.	List	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer:analyzer:deleteResourceConfigurations	Grants permission to delete resource configurations.	Write	analyzer *	g:ResourceTag/<tag-key>
AccessAnalyzer::validatePolicy	Grants permission to validate a policy.	Read	-	-
AccessAnalyzer::checkNoNewAccess	Grants permission to check if the updated policy has new access.	Read	-	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-245**, 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 IAM Access Analyzer.

Table 5-245 Resource types supported by IAM Access Analyzer

Resource Type	URN
analyzer	AccessAnalyzer:<region>:<account-id>:analyzer:<analyzer-id>

Resource Type	URN
archiveRule	AccessAnalyzer:<region>:<account-id>:archiveRule:<analyzer-id>/<archive-rule-id>

Conditions

IAM Access Analyzer 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.

5.10.13.13 Cloud Trace Service (CTS)

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.

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 edit 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 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 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 cts, see **Conditions**.

The following table lists the actions that you can define in SCP statements for cts.

Table 5-246 Actions supported by CTS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cts:trace:list	Grants permission to query audit traces.	list	-	-
cts:tracker:create	Grants permission to create a tracker.	write	-	-
cts:tracker:list	Grants permission to query trackers.	list	-	-
cts:tracker:update	Grants permission to update a tracker.	write	cts:<region>:<account-id>:tracker:<tracker-id>	-
cts:tracker:delete	Grants permission to delete a tracker.	write	cts:<region>:<account-id>:tracker:<tracker-id>	-
cts:quota:get	Grants permission to query tracker quotas.	read	-	-
cts:notification:create	Grants permission to create a notification rule.	write	-	-
cts:notification:update	Grants permission to update a key event notification.	write	cts:<region>:<account-id>:notification:<notification-id>	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
cts:notification:list	Grants permission to query key event notifications.	list	-	-
cts:notification:delete	Grants permission to delete a notification rule.	write	cts:<region>:<account-id>:notification:<notification-id>	-
cts:tag:create	Grants permission to create a resource tag.	tagging	cts:<region>:<account-id>:tracker:<tracker-id>	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
cts:tag:delete	Grants permission to delete a resource tag.	tagging	cts:<region>:<account-id>:tracker:<tracker-id>	-
			-	• g:TagKeys • g:RequestTag/<tag-key>
cts:notification:listOperation	Grants permission to query all operation lists.	list	-	-
cts:trace:listTraceUser	Grants permission to query all operator lists.	list	-	-
cts:trace:listResource	Grants permission to query all trace resource type lists.	list	-	-

Each API of cts usually supports one or more actions. **Table 5-247** lists the supported actions and dependencies.

Table 5-247 Actions and dependencies of CTS APIs

API	Action	Dependencies
GET /v3/{project_id}/traces	cts:trace:list	-
GET /v3/{project_id}/quotas	cts:quota:get	-
POST /v3/{project_id}/tracker	cts:tracker:create	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
PUT /v3/{project_id}/tracker	cts:tracker:update	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
GET /v3/{project_id}/trackers	cts:tracker:list	-
DELETE /v3/{project_id}/trackers	cts:tracker:delete	-
POST /v3/{project_id}/notifications	cts:notification:create	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups

API	Action	Dependencies
PUT /v3/{project_id}/notifications	cts:notification:update	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
DELETE /v3/{project_id}/notifications	cts:notification:delete	-
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
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	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
PUT /v3/{project_id}/tracker	cts:tracker:update	• lts:topics:list • lts:topics:create • lts:groups:list • lts:groups:create • obs:bucket:CreateBucket • obs:bucket:HeadBucket • obs:bucket:GetLifecycleConfiguration • obs:bucket:PutLifecycleConfiguration • obs:bucket:GetBucketAcl • obs:bucket:PutBucketAcl • kms:cmk:list
GET /v3/{project_id}/trackers	cts:tracker:list	-
DELETE /v3/{project_id}/trackers	cts:tracker:delete	-
POST /v3/{project_id}/notifications	cts:notification:create	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
PUT /v3/{project_id}/notifications	cts:notification:update	• smn:topic:listTopic • iam:users:listUsers • iam:groups:listGroups
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

CTS does not support resource-level authorization. To allow access to cts, use a wildcard (*) in the Resource element of the SCP, indicating that the SCP will be applied to all resources.

Conditions

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, cts:) only apply to operations of the CTS service. For details, see **Table 5-248**.
  - 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.

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 5-248 Service-specific condition keys supported by CTS

Condition Key	Type	Single-valued/ Multivalued	Description
cts:TargetType	string	Single-valued	Filter access permissions by data dump type.
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.

5.10.13.14 Resource Governance Center (RGC)

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 IAM custom identity policies and 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 (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 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 RGC, 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 RGC, see **Conditions**.

The following table lists the actions that you can define in SCP statements for RGC.

Table 5-249 Actions supported by RGC

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
rgc:control:list	Grants permission to list all governance policies.	List	-	-	-
rgc:controlViolation:list	Grants permission to list non-compliance.	List	-	-	-
rgc:control:get	Grants permission to get 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 query the status of a governance policy.	Read	-	-	-
rgc:enabledControl:list	Grants permission to list enabled governance policies.	List	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
rgc:controlsForOrganizationalUnit:list	Grants permission to list governance policies enabled for a registered OU.	List	-	-	-
rgc:controlsForAccount:list	Grants permission to list governance policies enabled for an enrolled account.	List	-	-	-
rgc:complianceStatusForAccount:get	Grants permission to query the resource compliance status of an enrolled account in an organization.	Read	-	-	-
rgc:complianceStatusForOrganizationalUnit:get	Grants permission to query the resource compliance status of all enrolled accounts under a registered OU in an organization.	Read	-	-	-
rgc:controlsForOrganizationalUnit:get	Grants permission to list governance policies enabled for an OU.	Read	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
rgc:controlsForAccount:get	Grants permission to list governance policies enabled for an account.	Read	-	-	-
rgc:configRuleCompliance:list	Grants permission to query the Config rule compliance for enrolled accounts.	List	-	-	-
rgc:externalConfigRuleCompliance:list	Grants permission to list the external Config rule compliance for enrolled accounts.	List	-	-	-
rgc:driftDetail:list	Grants permission to query drift details.	List	-	-	-
rgc:managedOrganizationalUnit:register	Grants permission to register an OU.	Write	-	-	-
rgc:managedOrganizationalUnit:reRegister	Grants permission to re-register an OU.	Write	-	-	-
rgc:managedOrganizationalUnit:deRegister	Grants permission to deregister an OU.	Write	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
rgc:operation:get	Grants permission to obtain registration information.	Read	-	-	-
rgc:managedOrganizationalUnit:delete	Grants permission to delete a registered OU.	Write	-	-	-
rgc:managedOrganizationalUnit:get	Grants permission to get details of a registered OU.	Read	-	-	-
rgc:managedOrganizationalUnit:create	Grants permission to create an OU.	Write	-	-	-
rgc:managedOrganizationalUnit:list	Grants permission to list registered OUs for which governance policies are enabled.	List	-	-	-
rgc:managedAccount:enroll	Grants permission to enroll an account.	Write	-	-	-
rgc:managedAccount:unEnroll	Grants permission to unmanage an account.	Write	-	-	-
rgc:managedAccount:update	Grants permission to update an enrolled account.	Write	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
rgc:managedAccount:get	Grants permission to get details of an enrolled account.	Read	-	-	-
rgc:managedAccountsForParent:list	Grants permission to list all enrolled accounts in a registered OU.	List	-	-	-
rgc:managedAccount:create	Grants permission to create an account.	Write	-	-	-
rgc:managedAccount:list	Grants permission to list enrolled accounts for which governance policies are enabled.	List	-	-	-
rgc:managedCoreAccount:get	Grants permission to get details of an enrolled core account.	Read	-	-	-
rgc:homeRegion:get	Grants permission to identify the home region.	Read	-	-	-
rgc:preLaunch:check	Grants permission to perform pre-checks before landing zone setup.	Write	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
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 query the landing zone setup status.	Read	-	-	-
rgc:availableUpdate:get	Grants permission to query the updateable status of a landing zone.	Read	-	-	-
rgc:landingZoneConfiguration:get	Grants permission to query landing zone settings.	Read	-	-	-
rgc:landingZoneIdentityCenter:get	Grants permission to obtain IAM Identity Center user information.	Read	-	-	-
rgc:operation:list	Grants permission to query the status of a registered OU or an enrolled account.	List	-	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key	Alias
rgc:templateDeployParam:get	Grants permission to obtain template deployment parameters.	Read	-	-	-
rgc:template:create	Grants permission to create a template.	Write	-	-	-
rgc:template:delete	Grants permission to delete a template.	Write	-	-	-
rgc:predefinedTemplate:list	Grants permission to list preset templates.	List	-	-	-
rgc:managedAccountTemplate:get	Grants permission to get details of a template for enrolled accounts.	Read	-	-	-

Each API of RGC usually supports one or more actions. **Table 5-250** lists the supported actions and dependencies.

Table 5-250 Actions and dependencies supported by RGC APIs

API	Action	Dependencies
POST /v1/governance/control/enable	rgc:control:enable	-
POST /v1/governance/control/disable	rgc:control:disable	-
GET /v1/governance/operated-controls/{control_operate_request_id}	rgc:controlOperate:get	-

API	Action	Dependencies
GET /v1/governance/managed-organizational-unit/{managed_organizational_unit_id}/controls	rgc:controlsForOrganizationalUnit:list	-

Resources

RGC does not support resource-specific permission control in SCPs. If you want to allow access to RGC, use the wildcard (*) for the Resource element to apply SCPs to all resources.

Conditions

RGC 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.

5.10.13.15 Application Operations Management (AOM)

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 AOM, 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 AOM, see **Conditions**.

The following table lists the actions that you can define in SCP statements for AOM.

Table 5-251 Actions supported by AOM

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aom:metric:delete	Grants permission to delete monitoring configurations.	write	-	-
aom:icmgr:get	Grants permission to query the collection component version list.	read	-	-
aom:agency:get	Grants permission to query agency permissions.	read	-	-
aom:icmgr:list	Grants permission to query the collection component version list.	list	-	-
aom:metric:list	Grants permission to query metrics.	list	-	-
aom:metric:put	Grants permission to report metrics.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aom:discoveryRule:set	Grants permission to create or update the service discovery rule list.	write	-	-
aom:discoveryRule:delete	Grants permission to delete the service discovery rule list.	write	-	-
aom:discoveryRule:list	Grants permission to query the service discovery rule list.	list	-	-
aom:alarmRule:create	Grants permission to create alarm rules.	write	alarmRule *	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
aom:alarmRule:list	Grants permission to query the alarm rule list.	list	-	-
aom:alarmRule:update	Grants permission to update alarm rules.	write	-	-
aom:alarmRule:delete	Grants permission to delete alarm rules.	write	alarmRule *	g:ResourceTag/<tag-key>
aom:alarm:put	Grants permission to report alarms and events.	write	-	-
aom:alarm:list	Grants permission to query alarms and events.	list	-	-
aom:alarmRule:get	Grants permission to query alarm rules.	read	-	-
aom:view:create	Grants permission to create a dashboard.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aom:event2AlarmRule:list	Grants permission to query the event alarm rule list.	list	-	-
aom:event2AlarmRule:create	Grants permission to create event alarm rules.	write	-	-
aom:event2AlarmRule:update	Grants permission to update event alarm rules.	write	-	-
aom:event2AlarmRule:delete	Grants permission to delete event alarm rules.	write	-	-
aom:muteRule:create	Grants permission to create silence rules.	write	-	-
aom:muteRule:list	Grants permission to query the silence rule list.	list	-	-
aom:muteRule:update	Grants permission to update silence rules.	write	-	-
aom:muteRule:delete	Grants permission to delete silence rules.	write	-	-
aom:actionRule:get	Grants permission to query action rules.	read	-	-
aom:actionRule:list	Grants permission to query the action rule list.	list	-	-
aom:actionRule:create	Grants permission to create action rules.	write	-	-
aom:actionRule:update	Grants permission to modify action rules.	write	-	-

Action	Description	Access Level	Resource Type (*: Required)	Condition Key
aom:actionRule:delete	Grants permission to delete action rules.	write	-	-

Each API of AOM usually supports one or more actions. **Table 5-252** lists the supported actions and dependencies.

Table 5-252 Actions and dependencies supported by AOM APIs

API	Action	Dependencies
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	-
POST /v1/{project_id}/{prometheus_instance}/aom/api/v1/rules	aom:metric:put	-
GET /v1/{project_id}/access-code	aom:icmgr:get	-
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	-

API	Action	Dependencies
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	-
POST /v1/{project_id}/ams/metricdata	aom:metric:list	-
POST /v1/{project_id}/ams/report/metricdata	aom:metric:put	-
PUT /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:set	-

API	Action	Dependencies
DELETE /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:delete	-
GET /v1/{project_id}/inv/servicediscoveryrules	aom:discoveryRule:list	-
POST /v2/{project_id}/alarm-rules	aom:alarmRule:create	-
GET /v2/{project_id}/alarm-rules	aom:alarmRule:list	-
PUT /v2/{project_id}/alarm-rules	aom:alarmRule:update	-
DELETE /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:delete	-
GET /v2/{project_id}/alarm-rules/{alarm_rule_id}	aom:alarmRule:get	-
POST /v2/{project_id}/alarm-rules/delete	aom:alarmRule:delete	-
POST /v2/{project_id}/events	aom:alarm:list	-
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	-

API	Action	Dependencies
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	-
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	-

API	Action	Dependencies
GET /v4/{project_id}/alarm-rules	aom:alarmRule:list	-
DELETE /v4/{project_id}/alarm-rules	aom:alarmRule:delete **NOTE** The resource type **alarmRule** of this action applies only to the **DELETE /v4/*{project_id}*/alarm-rules** API.	-

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-253**, 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 AOM.

Table 5-253 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 an SCP.

It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.13.16 Cloud Eye (CES)

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 topic 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 Cloud Eye, 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 Cloud Eye, see **Conditions**.

The following table lists the actions that you can define in SCP statements for Cloud Eye.

Table 5-254 Actions supported by Cloud Eye

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:widgets:put	Grants permission to batch update graphs.	write	dashboard	-
ces:widgets:create	Grants permission to create a graph.	write	dashboard	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:widgets:put	Grants permission to update a graph.	write	dashboard	-
ces:widgets:delete	Grants permission to delete a graph.	write	dashboard	-
ces:dashboards:create	Grants permission to create a dashboard.	write	dashboard	g:EnterpriseProjectId
ces:dashboards:list	Grants permission to query dashboards.	list	dashboard	g:EnterpriseProjectId
ces:dashboards:put	Grants permission to update a dashboard.	write	dashboard	g:EnterpriseProjectId
ces:widgets:list	Grants permission to query graphs added to a dashboard.	list	dashboard	-
ces:widgets:create	Grants permission to add a graph to a dashboard.	write	dashboard	-
ces:dashboards:delete	Grants permission to batch delete dashboards.	write	dashboard	g:EnterpriseProjectId
ces:widgets:get	Grants permission to query a graph.	read	dashboard	-
ces:dashboards:delete	Grants permission to delete a dashboard.	write	dashboard	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:metrics:list	Grants permission to query metrics.	list	-	-
ces:metricData:get	Grants permission to query a metric.	read	-	-
ces:metricData:create	Grants permission to report metrics.	write	-	-
ces:namespacesDimensions:listAgentDimensions	Grants permission to query Agent-related metrics of a server.	list	-	-
ces:namespacesDimensions:list	Grants permission to query dimensions of a cloud service.	list	-	-
ces:metaData:get	Grants permission to batch query metadata of dimensions.	read	-	-
ces:metricData:list	Grants permission to batch query metric data.	list	-	-
ces:namespacesDimensions:list	Grants permission to query metric data of top *N* resources from a specific dimension.	list	-	-
ces:alarms:list	Grants permission to query alarm rules.	list	alarm	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:alarms:create	Grants permission to create an alarm rule.	write	alarm	g:EnterpriseProjectId
ces:alarms:put	Grants permission to update an alarm rule.	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:get	Grants permission to query an alarm rule.	read	alarm	g:EnterpriseProjectId
ces:alarms:putAction	Grants permission to enable or disable an alarm rule.	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:delete	Grants permission to batch delete alarm rules.	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:listOneClickAlarms	Grants permission to query services and resources that support one-click monitoring.	list	alarm	g:EnterpriseProjectId
ces:alarms:putOneClickAlarms	Grants permission to modify alarm notifications for an alarm rule in one-click monitoring.	write	alarm	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:alarms:list	Grants permission to query alarm rules.	list	alarm	g:EnterpriseProjectId
ces:alarms:create	Grants permission to create an alarm rule.	write	alarm	g:EnterpriseProjectId
ces:alarms:putAlarmNotifications	Grants permission to modify alarm notification information in an alarm rule.	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:getPolicies	Grants permission to query policies in an alarm rule.	read	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:updatePolicies	Grants permission to update policies of an alarm rule.	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:getResources	Grants permission to query monitored resources in an alarm rule.	read	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:alarms:addResources	Grants permission to batch add resources to an alarm rule.	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:deleteResources	Grants permission to batch delete resources from an alarm rule.	write	alarm	• g:EnterpriseProjectId • g:ResourceTag/<tag-key>
ces:alarms:putNotificationMaskRules	Grants permission to modify an alarm notification masking rule.	write	alarm	g:EnterpriseProjectId
ces:alarms:listNotificationMaskResources	Grants permission to query resources for which alarm notifications have been masked.	list	alarm	g:EnterpriseProjectId
ces:alarms:deleteNotificationMaskRules	Grants permission to batch delete alarm notification masking rules.	write	alarm	g:EnterpriseProjectId
ces:alarms:listNotificationMaskRules	Grants permission to batch query alarm notification masking rules.	list	alarm	g:EnterpriseProjectId
ces:alarms:createOneClickAlarms	Grants permission to enable one-click monitoring.	write	alarm	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:alarms:putOneClickAlarmPolicies	Grants permission to batch enable or disable alarm policies in alarm rules for one service that has one-click monitoring enabled.	write	alarm	g:EnterpriseProjectId
ces:alarms:putOneClickAlarmNotifications	Grants permission to batch modify alarm notifications for one service in one-click monitoring.	write	alarm	g:EnterpriseProjectId
ces:alarms:deleteOneClickAlarms	Grants permission to batch disable one-click monitoring.	write	alarm	g:EnterpriseProjectId
ces:alarms:list	Grants permission to query alarms.	list	alarm	g:EnterpriseProjectId
ces:alarmHistory:list	Grants permission to query alarm records.	list	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:create	Grants permission to create a custom alarm template.	write	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:delete	Grants permission to delete a custom alarm template.	write	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:list	Grants permission to query custom alarm templates.	list	alarm	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:customAlarmTemplates:listAssociatedAlarms	Grants permission to query alarm rules associated with a custom alarm template.	read	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:put	Grants permission to update a custom alarm template.	write	alarm	g:EnterpriseProjectId
ces:quotas:get	Grants permission to query a quota.	read	-	-
ces:quotas:get	Grants permission to query quotas.	read	-	-
ces:events:get	Grants permission to query details of an event.	read	-	-
ces:events:list	Grants permission to query events.	list	-	-
ces:agent:listTaskInvocations	Grants permission to batch query Agent tasks of a server.	list	-	-
ces:agent:createAgentInvocations	Grants permission to batch create Agent tasks.	write	-	-
ces:events:post	Grants permission to report events.	write	-	-
ces:resourceGroups:addResources	Grants permission to batch add resources to a resource group.	write	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:resourceGroups:create	Grants permission to create a resource group.	write	-	g:EnterpriseProjectId
ces:resourceGroups:delete	Grants permission to delete a resource group.	write	-	g:EnterpriseProjectId
ces:resourceGroups:deleteResources	Grants permission to batch delete resources from a resource group.	write	-	g:EnterpriseProjectId
ces:resourceGroups:get	Grants permission to query a resource group.	read	-	g:EnterpriseProjectId
ces:resourceGroups:getServiceResources	Grants permission to query resources of a specified dimension and a specified service type in a resource group.	read	-	g:EnterpriseProjectId
ces:resourceGroups:put	Grants permission to update a resource group.	write	-	g:EnterpriseProjectId
ces:tags:list	Grants permission to batch query Cloud Eye tags.	list	-	-
ces:eventData:get	Grants permission to query the server configuration.	list	-	-
ces:resourceGroups:list	Grants permission to query all resource groups.	list	-	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
ces:resourceGroups:get	Grants permission to query a resource group.	read	-	g:EnterpriseProjectId
ces:customAlarmTemplates:list	Grants permission to query custom alarm templates.	list	alarm	g:EnterpriseProjectId
ces:customAlarmTemplates:get	Grants permission to query a custom alarm template.	read	alarm	g:EnterpriseProjectId
ces:alarms:create	Grants permission to create an alarm rule.	write	alarm	g:EnterpriseProjectId
ces:dashboards:put	Grants permission to update a cloud service dashboard.	write	dashboard	-
ces:namespacesDimensions:list	Grants permission to query metric data of top *N* resources from a specific dimension.	list	-	-
ces:namespacesDimensions:list	Grants permission to query dimensions of a cloud service.	list	-	-

Each API of Cloud Eye usually supports one or more actions. **Table 5-255** lists the supported actions and dependencies.

Table 5-255 Actions and dependencies supported by Cloud Eye APIs

API	Action	Dependencies
POST /v2/{project_id}/dashboards	ces:dashboards:create	-
GET /v2/{project_id}/dashboards	ces:dashboards:list	-
PUT /v2/{project_id}/dashboards/{dashboard_id}	ces:dashboards:put	-
GET /v2/{project_id}/dashboards/{dashboard_id}/widgets	ces:widgets:list	-
POST /v2/{project_id}/dashboards/{dashboard_id}/widgets	ces:widgets:create	-
POST /v2/{project_id}/dashboards/batch-delete	ces:dashboards:delete	-
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 /V1.0/{project_id}/metrics	ces:metrics:list	-
GET /V1.0/{project_id}/metric-data	ces:metricData:get	ces:metricData:list
POST /V1.0/{project_id}/metric-data	ces:metricData:create	-
POST /V1.0/{project_id}/batch-query-metric-data	ces:metricData:list	-
GET /v2/{project_id}/instances/{instance_id}/agent-dimensions	ces:namespacesDimensions:listAgentDimensions	ces:namespacesDimensions:list
GET /V1.0/{project_id}/alarms	ces:alarms:list	-
POST /V1.0/{project_id}/alarms	ces:alarms:create	-
PUT /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:put	ces:alarmsonoff:put
DELETE /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:delete	-

API	Action	Dependencies
GET /V1.0/{project_id}/alarms/{alarm_id}	ces:alarms:get	ces:alarms:list
PUT /V1.0/{project_id}/alarms/{alarm_id}/action	ces:alarms:putAction	ces:alarms:put
GET /v2/{project_id}/alarms	ces:alarms:list	-
POST /v2/{project_id}/alarms	ces:alarms:create	-
PUT /v2/{project_id}/alarms/{alarm_id}/notifications	ces:alarms:putAlarmNotifications	ces:alarms:put
GET /v2/{project_id}/alarms/{alarm_id}/policies	ces:alarms:getPolicies	ces:alarms:get
PUT /v2/{project_id}/alarms/{alarm_id}/policies	ces:alarms:updatePolicies	ces:alarms:put
GET /v2/{project_id}/alarms/{alarm_id}/resources	ces:alarms:getResources	-
POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-create	ces:alarms:addResources	ces:alarms:put
POST /v2/{project_id}/alarms/{alarm_id}/resources/batch-delete	ces:alarms:delete	ces:alarms:put
POST /v2/{project_id}/alarms/action	ces:alarms:putAction	ces:alarms:put
PUT /v2/{project_id}/notification-masks	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update
PUT /v2/{project_id}/notification-masks/{notification_mask_id}	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update
GET /v2/{project_id}/notification-masks/{notification_mask_id}/resources	ces:alarms:listNotificationMaskResources	ces:notificationMasks:list
POST /v2/{project_id}/notification-masks/batch-delete	ces:alarms:deleteNotificationMaskRules	ces:notificationMasks:delete
POST /v2/{project_id}/notification-masks/batch-query	ces:alarms:listNotificationMaskRules	ces:notificationMasks:list
POST /v2/{project_id}/notification-masks/batch-update	ces:alarms:putNotificationMaskRules	ces:notificationMasks:update

API	Action	Dependencies
GET /v2/{project_id}/one-click-alarms	ces:alarms:listOneClickAlarms	ces:oneClickAlarms:list
POST /v2/{project_id}/one-click-alarms	ces:alarms:createOneClickAlarms	ces:oneClickAlarms:post
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarm-rules/action	ces:alarms:putOneClickAlarms	ces:oneClickAlarms:put
GET /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms	ces:alarms:listOneClickAlarms	ces:oneClickAlarms:list
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/alarms/{alarm_id}/policies/action	ces:alarms:putOneClickAlarmPolicies	ces:oneClickAlarms:put
PUT /v2/{project_id}/one-click-alarms/{one_click_alarm_id}/notifications	ces:alarms:putOneClickAlarmNotifications	ces:oneClickAlarms:updateNotifications
POST /v2/{project_id}/one-click-alarms/batch-delete	ces:alarms:deleteOneClickAlarms	ces:oneClickAlarms:delete
POST /v2/{project_id}/alarms/batch-delete	ces:alarms:deleteResources	ces:alarms:put
GET /V1.0/{project_id}/alarm-histories	ces:alarmHistory:list	-
GET /v2/{project_id}/alarm-histories	ces:alarmHistory:list	-
POST /V1.0/{project_id}/alarm-template	ces:customAlarmTemplates:create	-
POST /v2/{project_id}/alarm-templates	ces:customAlarmTemplates:create	-
DELETE /V1.0/{project_id}/alarm-template/{template_id}	ces:customAlarmTemplates:delete	-
POST /v2/{project_id}/alarm-templates/batch-delete	ces:customAlarmTemplates:delete	-
GET /v2/{project_id}/alarm-templates/{template_id}	ces:customAlarmTemplates:get	ces:customAlarmTemplates:list
GET /V1.0/{project_id}/alarm-template	ces:customAlarmTemplates:list	-
GET /v2/{project_id}/alarm-templates	ces:customAlarmTemplates:list	-

API	Action	Dependencies
GET /v2/{project_id}/alarm-templates/{template_id}/association-alarms	ces:customAlarmTemplates:listAssociatedAlarms	ces:customAlarmTemplates:list
PUT /V1.0/{project_id}/alarm-template/{template_id}	ces:customAlarmTemplates:put	-
PUT /v2/{project_id}/alarm-templates/{template_id}	ces:customAlarmTemplates:put	-
GET /V1.0/{project_id}/quotas	ces:quotas:get	-
GET /V1.0/{project_id}/event/{event_name}	ces:events:get	-
GET /V1.0/{project_id}/events	ces:events:list	-
GET /v3/{project_id}/agent-invocations	ces:agent:listTaskInvocations	ces:taskInvocation:get
POST /v3/{project_id}/agent-invocations/batch-create	ces:agent:createAgentInvocations	ces:taskInvocation:post
POST /V1.0/{project_id}/events	ces:events:post	-
POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-create	ces:resourceGroups:addResources	ces:resourceGroups:put
POST /V1.0/{project_id}/resource-groups	ces:resourceGroups:create	-
POST /v2/{project_id}/resource-groups	ces:resourceGroups:create	-
DELETE /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:delete	-
POST /v2/{project_id}/resource-groups/batch-delete	ces:resourceGroups:delete	-
POST /v2/{project_id}/resource-groups/{group_id}/resources/batch-delete	ces:resourceGroups:deleteResources	ces:resourceGroups:put
GET /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:get	-
GET /v2/{project_id}/resource-groups/{group_id}	ces:resourceGroups:get	-
GET /v2/{project_id}/resource-groups/{group_id}/services/{service}/resources	ces:resourceGroups:getServiceResources	ces:resourceGroups:get

API	Action	Dependencies
GET /V1.0/{project_id}/resource-groups	ces:resourceGroups:list	ces:resourceGroups:get
GET /v2/{project_id}/resource-groups	ces:resourceGroups:list	ces:resourceGroups:get
PUT /V1.0/{project_id}/resource-groups/{group_id}	ces:resourceGroups:put	-
PUT /v2/{project_id}/resource-groups/{group_id}	ces:resourceGroups:put	-
GET /v2/{project_id}/{resource_type}/tags	ces:tags:list	-
GET /V1.0/{project_id}/event-data	ces:eventData:get	ces:sapEventData:list
POST /v3/{project_id}/agent-status/batch-query	ces:agent:listStatuses	-

Resources

A resource type indicates the resources that an SCP is applied. If you specify a resource type for any action in **Table 5-256**, 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 policy to define resource types.

The following table lists the resource types that you can specify in SCP statements for Cloud Eye.

Table 5-256 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

Cloud Eye does not support service-specific condition keys in an SCP.

It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.13.17 IAM Identity Broker

Organizations 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.

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 IAM Identity Broker, 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 IAM Identity Broker, see **Conditions**.

The following table lists the actions that you can define in policy statements for IAM Identity Broker.

Table 5-257 Actions supported by IAM Identity Broker

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AgenciesAnywhere:trustAnchor:create	Grants permission to create a trust anchor.	Write	-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere:trustAnchor:enable	Grants permission to enable a trust anchor.	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:disable	Grants permission to disable a trust anchor.	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:update	Grants permission to modify a trust anchor.	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:get	Grants permission to query details about a trust anchor.	Read	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:list	Grants permission to list trust anchors.	List	-	-
AgenciesAnywhere:trustAnchor:delete	Grants permission to delete a trust anchor.	Write	trustAnchor *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:putNotificationSettings	Grants permission to set notification settings for a trust anchor.	Write	trustAnchor *	g:ResourceTag/<tag-key>
AgenciesAnywhere:trustAnchor:resetNotificationSettings	Grants permission to reset the notification settings for a trust anchor.	Write	trustAnchor *	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AgenciesAnywhere:profile:create	Grants permission to create a profile.	Write	-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere:profile:enable	Grants permission to enable a profile.	Write	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:disable	Grants permission to disable a profile.	Write	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:update	Grants permission to modify a profile.	Write	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:get	Grants permission to query profile details.	Read	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:profile:list	Grants permission to list profiles.	List	-	-
AgenciesAnywhere:profile:delete	Grants permission to delete a profile.	Write	profile *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere::listResourcesByTag	Grants permission to list resources or the resource quantity by tag.	List	-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere::tagResource	Grants permission to tag a specified resource.	Tagging	trustAnchor	g:ResourceTag/<tag-key>
			profile	g:ResourceTag/<tag-key>
			crl	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AgenciesAnywhere::unTagResource	Grants permission to untag a specified resource.	Tagging	trustAnchor	g:ResourceTag/<tag-key>
			profile	g:ResourceTag/<tag-key>
			crl	g:ResourceTag/<tag-key>
			-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere::listTagsForResource	Grants permission to list the tags of a specified resource.	List	profile	g:ResourceTag/<tag-key>
			crl	g:ResourceTag/<tag-key>
			trustAnchor	g:ResourceTag/<tag-key>
AgenciesAnywhere::listTags	Grants permission to list resource tags.	List	-	-
AgenciesAnywhere:crl:import	Grants permission to import a certificate revocation list.	Write	-	• g:TagKeys • g:RequestTag/<tag-key>
AgenciesAnywhere:crl:enable	Grants permission to enable a certificate revocation list.	Write	crl *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:disable	Grants permission to disable a certificate revocation list.	Write	crl *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:update	Grants permission to update a certificate revocation list.	Write	crl *	-
			-	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:get	Grants permission to query a certificate revocation list.	Read	crl *	-
			-	g:ResourceTag/<tag-key>

Action	Description	Access Level	Resource Type (*: required)	Condition Key
AgenciesAnywhere:crl:list	Grants permission to list the certificate revocation lists.	List	-	-
AgenciesAnywhere:crl:listForTrustAnchor	Grants permission to list the certificate revocation lists of a specified trust anchor.	List	trustAnchor *	g:ResourceTag/<tag-key>
AgenciesAnywhere:crl:delete	Grants permission to delete a certificate revocation list.	Write	crl *	-
			-	g:ResourceTag/<tag-key>

Resources

A resource type indicates the resources that an SCP applies to. If you specify a resource type for any action in **Table 5-258**, 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 IAM Identity Broker.

Table 5-258 Resources supported by IAM Identity Broker

Resource	URN
profile	AgenciesAnywhere::<account-id>:profile:<profile-id>
crl	AgenciesAnywhere::<account-id>:crl:<crl-id>
trustAnchor	AgenciesAnywhere::<account-id>:trustAnchor:<trust-anchor-id>

Conditions

IAM Identity Broker 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.

5.10.14 User Support

5.10.14.1 Billing Center

The Organizations service 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.

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 edit a custom SCP policy, 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.
- 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.

The following table lists the actions that you can define in SCPs for the Billing Center.

Table 5-259 Supported actions

Action	Description	Access Level	Resource Type	Condition Key
billing:balance:update	Grants the permission to withdraw money, top up the account, make payments, and enable the balance alerting.	write	-	-
billing:balance:view	Grants the permission to view account statements, payment records, expenditure quotas, accounting adjustment records, and arrears.	list	-	g:EnterpriseProjectId
billing:bill:update	Grants the permission to set bills.	write	-	-
billing:bill:view	Grants the permission to view bills, expenditures of the current month, and expenditure growth.	list	-	g:EnterpriseProjectId
billing:resourcePackages:view	Grants the permission to view resource packages, remaining resources, and resource usage, and to export the resource usage details.	list	-	-
billing:resourcePackages:update	Grants the permission to set alerts for remaining resources in resource packages.	write	-	-
billing:billDetail:update	Grants the permission to set bill details.	write	-	g:EnterpriseProjectId
billing:billDetail:view	Grants the permission to view bill details.	read	-	g:EnterpriseProjectId
billing:contract:update	Grants the permission to view offline contracts.	write	-	-
billing:coupon:view	Grants the permission to view and activate coupons.	read	-	-
billing:contract:viewDiscount	Grants the permission to view commercial discounts.	read	-	-
billing:invoice:manage	Grants the permission to manage invoices.	write	-	-
billing:invoice:view	Grants the permission to view invoice records and details.	read	-	-
billing:invoice:export	Grants the permission to export invoice information and download invoices.	read	-	-

Action	Description	Access Level	Resource Type	Condition Key
billing:order:pay	Grants the permission to pay for the orders.	write	-	g:EnterpriseProjectId
billing:order:view	Grants the permission to view order information and pay-per-usage resource packages.	list	-	g:EnterpriseProjectId
billing:subscription:renew	Grants the 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 the permission to view renewable subscriptions and query the resources that can be changed from pay-per-use to yearly/monthly.	list	-	g:EnterpriseProjectId
billing:subscription:unsubscribe	Grants the permission to view the resources that can be unsubscribed from and have been unsubscribed from.	write	-	g:EnterpriseProjectId
billing:bill:export	Grants the permission to export the bill summary.	read	-	g:EnterpriseProjectId
billing:billDetail:export	Grants the permission to export the bill details.	read	-	g:EnterpriseProjectId
billing:balance:export	Grants the permission to export the transaction and payment records.	read	-	-
billing:consumption:view	Grants the permission to view expenditure breakdown by enterprise project.	read	-	-
billing::activeEPFinance	Grants the permission to enable Enterprise Project.	write	-	-
billing::activeEPFundQuota	Grants the permission to enable or disable the fund quota function for enterprise projects.	write	-	-
billing::viewEPFundQuota	Grants the permission to query the fund quota of an enterprise project.	read	-	-
billing::updateEPFundQuota	Grants the permission to modify the fund quota of an enterprise project.	write	-	-

Action	Description	Access Level	Resource Type	Condition Key
billing::listEPFundQuotaHistory	Grants the permission to view the fund quota adjustment records of enterprise projects.	read	-	-
billing::updateEPGroup	Grants the permission to modify the enterprise project groups.	write	-	-
billing::viewEPGroup	Grants the permission to view enterprise project groups.	read	-	-

Resources

Billing Center does not support resource-specific permission control in SCPs. If you want to allow access to Billing Center, use the wildcard (*) for the Resource element to apply SCPs to all resources.

Conditions

Billing Center 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.

5.10.14.2 Cost Center

The Organizations service 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.

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 edit a custom SCP policy, 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 (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 SCP.
- The **Resource Type** column indicates whether the action supports resource-level permissions. Actions supported by Cost Center are valid for all resources. You can use a wildcard (*) to indicate all resource types.

  - 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.
- 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.

The following table lists the actions that you can define in SCPs for Cost Center.

Table 5-260 Supported actions

Action	Description	Access Level	Resource Type	Condition Key
costCenter:costAnalysis:listCosts	Grants permission to view cost analysis.	read	-	-
costCenter:costAnalysis:configReport	Grants permission to manage cost reports, including creating, modifying, and deleting custom reports.	write	-	-
costCenter:costAnalysis:listReports	Grants permission to view a list of cost reports.	read	-	-
costCenter:costDetail:listCostDetails	Grants permission to view cost details.	read	-	-
costCenter:budget:configBudget	Grants permission to manage budgets, including creating, modifying, and deleting budgets.	write	-	-
costCenter:budget:viewBudget	Grants permission to view budget information, including the budget list and budget details.	read	-	-

Action	Description	Access Level	Resource Type	Condition Key
costCenter:budget:deleteBudgetReport	Grants permission to delete a budget report.	write	-	-
costCenter:budget:configBudgetReport	Grants permission to add and modify a budget report.	write	-	-
costCenter:budget:viewBudgetReport	Grants permission to view budget reports, including the budget list and budget details.	read	-	-
costCenter:costAnomalyDetection:deleteMonitor	Grants permission to delete a cost monitor.	write	-	-
costCenter:costAnomalyDetection:configMonitor	Grants permission to add and edit a cost monitor.	write	-	-
costCenter:costAnomalyDetection:viewMonitor	Grants permission to view cost monitors and anomalies.	read	-	-
costCenter:costAnomalyDetection:configMonitorAlert	Grants permission to configure alerting for cost anomalies.	write	-	-
costCenter:costAnomalyDetection:viewMonitorAlert	Grants permission to view cost anomaly alerts.	read	-	-
costCenter:costAnomalyDetection:provideFeedback	Grants permission to provide feedback on cost anomalies.	read	-	-
costCenter:recommendation:viewRecommendationSummary	Grants permission to view the summary of cost optimization recommendations.	read	-	-

Action	Description	Access Level	Resource Type	Condition Key
costCenter:recommendation:viewRecommendationSubscription	Grants permission to query subscriptions to cost optimization recommendations.	read	-	-
costCenter:recommendation:configRecommendationSubscription	Grants permission to configure or delete subscriptions to cost optimization recommendations.	write	-	-
costCenter:recommendation:viewYearlyMonthlyRecommendation	Grants permission to view the cost optimization option of changing pay-per-use to yearly/monthly.	read	-	-
costCenter:recommendation:viewResourcePkgRecommendation	Grants permission to view resource package purchase recommendations.	read	-	-
costCenter:recommendation:viewResourceOptimizeRecommendation	Grants permission to view optimization recommendations for idle resources.	read	-	-
costCenter:recommendation:configPreference	Grants permission to define idle resource identifying rules.	write	-	-
costCenter:costTag:updateStatus	Grants permission to activate or deactivate cost tags.	write	-	-
costCenter:costTag:listCostTags	Grants permission to view cost tags.	read	-	-
costCenter:costCategory:deleteCostCategory	Grants permission to delete cost categories.	write	-	-
costCenter:costCategory:configCostCategory	Grants permission to configure cost categories, including creating and editing cost categories.	write	-	-

Action	Description	Access Level	Resource Type	Condition Key
costCenter:costCategory:viewCostCategory	Grants permission to view cost category information, including the cost category list and the details of each cost category.	read	-	-
costCenter:resourcePackage:viewResourcePkgAnalysis	Grants permission to view the analysis of resource package utilization and coverage.	read	-	-
costCenter:savingsPlans:viewSavingsPlansAnalysis	Grants permission to view the analysis of savings plan utilization and coverage.	read	-	-
costCenter:reserveInstance:viewRIAnalysis	Grants permission to view the analysis of reserved instance utilization and coverage.	read	-	-
costCenter:savingsPlans:viewSavingsPlans	Grants permission to view savings plans.	read	-	-
costCenter:recommendation:viewSavingsPlansRecommendation	Grants permission to view savings plans purchase recommendations.	read	-	-
costCenter::updateCostConfig	Grants permission to enable Cost Center functions.	write	-	-
costCenter:preference:delete	Grants permission to disable Cost Center functions.	write	-	-
costCenter:costdetailreport:viewReportTask	Grants permission to view the task list for exporting cost details to OBS.	read	-	-
costCenter:costdetailreport:configReportTask	Grants permission to create, modify, or delete the tasks for exporting cost details to OBS.	write	-	-
costCenter:helper:listCostAllocations	Grants permission to view the percentage of allocated costs.	list	-	-

Action	Description	Access Level	Resource Type	Condition Key
costCenter:helper:viewCostRating	Grants permission to view cost allocation maturity rating.	read	-	-

Resources

Cost Center does not support resource-specific permission control in SCPs. If you want to allow access to Cost Center, use the wildcard (*) for the Resource element to apply SCPs to all resources.

Conditions

Cost Center 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.

5.10.14.3 My Account

The Organizations service provides Service Control Policies (SCPs) for access control.

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 only 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 edit a custom SCP policy, 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. Actions supported by Account Center are valid for all resources. You can use a wildcard (*) to indicate all resource types.
  - 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.
- 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.

The following table lists the actions that you can define in SCPs for Account Center.

Table 5-261 Supported actions

Action	Description	Access Level	Resource Type (*: required)	Condition Key
account:accountInfo:update	Grants permission to update account information, including real-name authentication, basic information, and preferences.	Write	-	-
account:cps:view	Grants permission to view the promotion data of Recommendations and Rebates by cloud promoters.	Read	-	-
account:cps:update	Grants permission to join the reward promotion program.	Write	-	-
account:privilege:view	Grants permission to view my privileges and prizes.	Read	-	-
account::close	Grants permission to close, disable, and restore Huawei Cloud services.	Write	-	-

Resources

Account Center does not support resource-specific permission control in SCPs. If you want to allow access to Account Center, use the wildcard (*) for the Resource element to apply SCPs to all resources.

Conditions

Account Center 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.

5.10.14.4 Enterprise Center

SCPs allow you to use the elements described below.

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 edit a custom SCP policy, 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. Actions supported by Enterprise Center are valid for all resources. You can use a wildcard (*) to indicate all resource types.
  - 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.
- 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.

The following table lists the actions that you can define in SCPs for Enterprise Center.

Table 5-262 Supported actions

Action	Description	Access Level	Resource Type (*: required)	Condition Key
businessUnitCenter:bill:update	Grants permission to perform operations 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	-	-
businessUnitCenter:businessUnit:update	Grants permission to modify organizations and accounts.	Write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
businessUnitCenter:businessUnit:view	Grants permission to view organizations and accounts.	Read	-	-
businessUnitCenter:businessUnitBudget:update	Grants permission to perform operations on organization budgets.	Write	-	-
businessUnitCenter:businessUnitBudget:view	Grants permission to view organization budgets.	Read	-	-
businessUnitCenter:businessUnitPolicy:update	Grants permission to modify organization policies.	Write	-	-
businessUnitCenter::active	Grants permission to enable and disable Enterprise Center.	Write	-	-

Resources

Enterprise Center does not support resource-specific permission control in SCPs. If you need to allow access to Enterprise Center, use the wildcard (*) for the Resource element to apply SCPs to all resources.

Conditions

Enterprise Center 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.

5.10.14.5 Message Center

The Organizations service 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.

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 edit a custom SCP policy, 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. Actions supported by Message Center are valid for all resources. You can use a wildcard (*) to indicate all resource types.
- 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.

The following table lists the actions that you can define in SCPs for Message Center.

Table 5-263 Supported actions

Action	Grants Permission To	Access Level	Resource Type (*: required)	Condition Key
messageCenter:financeMsg:view	• View, mark, and delete financial messages. • View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A

Action	Grants Permission To	Access Level	Resource Type (*: required)	Condition Key
messageCenter:financeMsg:subscribe	• View settings on the **SMS & Email Settings** and **Voice Settings** pages. • Modify the message receiving method for financial messages.	write	*	N/A
messageCenter:financeMsg:delete	• View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:filingMsg:view	• View, mark, and delete filing messages. • View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:filingMsg:subscribe	• View settings on the **SMS & Email Settings** and **Voice Settings** pages. • Modify the message receiving method for filing messages.	write	*	N/A
messageCenter:filingMsg:delete	• View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:contractMsg:view	• View, mark, and delete contract and commerce messages. • View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:contractMsg:subscribe	• View settings on the **SMS & Email Settings** and **Voice Settings** pages. • Modify the message receiving method for contract and commerce messages.	write	*	N/A
messageCenter:contractMsg:delete	• View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:campaignsMsg:view	• View, mark, and delete campaign messages. • View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:campaignsMsg:subscribe	• View settings on the **SMS & Email Settings** and **Voice Settings** pages. • Modify the message receiving method for campaign messages.	write	*	N/A
messageCenter:campaignsMsg:delete	• View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A

Action	Grants Permission To	Access Level	Resource Type (*: required)	Condition Key
messageCenter:productMsg:view	• View, mark, and delete product messages. • View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:productMsg:subscribe	• View settings on the **SMS & Email Settings** and **Voice Settings** pages. • Modify the message receiving method for product messages.	write	*	N/A
messageCenter:productMsg:delete	• View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:omMsg:view	• View, mark, and delete O&M messages. • View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:omMsg:subscribe	• View settings on the **SMS & Email Settings** and **Voice Settings** pages. • Modify the message receiving method for O&M messages.	write	*	N/A
messageCenter:omMsg:delete	• View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:securityMsg:view	• View, mark, and delete security messages. • View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:securityMsg:subscribe	• View settings on the **SMS & Email Settings** and **Voice Settings** pages. • Modify the message receiving method for security messages.	write	*	N/A
messageCenter:securityMsg:delete	• View settings on the **SMS & Email Settings** and **Voice Settings** pages.	read	*	N/A
messageCenter:recipient:view	• View settings on the **SMS & Email Settings** and **Recipient Management** pages.	read	*	N/A
messageCenter:recipient:update	• View settings on the **SMS & Email Settings** page. Add recipients on the **Recipient Management** page. (This action must be used together with **messageCenter:recipient:view**.)	write	*	N/A

Resources

Message Center does not support resource-specific permission control in SCPs. If you want to allow access to Message Center, use the wildcard (*) for the Resource element to apply SCPs to all resources.

Conditions

Message Center 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.

5.10.14.6 Customer Operation Capabilities

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 IAM custom identity policies and 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 Business Support System (BSS), 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 BSS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for BSS.

Table 5-264 Actions supported by BSS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
billing:contract:viewDiscount	Grants the permission to view discounts.	read	-	-
billing:balance:view	Grants the permission to view account statements, payment records, expenditure quotas, bill adjustment records, and arrears.	list	-	-
billing:coupon:view	Grants the permission to view coupons and stored-value cards and activate coupons.	read	-	-
billing:order:view	Grants the permission to view order information and pay-per-usage packages.	list	-	-
billing:order:pay	Grants the permission to pay for orders.	write	-	-
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	Grant the permission to view resources that can be or has been unsubscribed from, cancel delivery, and return or replace hardware.	write	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
billing:resourcePackages:view	Grants the permission to view resource packages, view resource package usage, and query and export usage details.	list	-	-
billing:billDetail:view	Grants the permission to view bill 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::activeEPFinance	Grants the permission to enable the enterprise project function.	write	-	-
businessUnitCenter:businessUnit:view	Grants the permission to view organizations and accounts.	read	-	-
billing:invoice:update	Grants the permission to manage invoices, request invoices, and manage invoice titles and addresses.	write	-	-

Each API usually supports one or more actions. **Table 5-265** lists supported actions and their dependencies.

Table 5-265 APIs and actions (APIs listed do not require any dependency.)

Scenario	Sub-Scenario	API	API URL	Action	Action Description
Managing products	Querying product price	Querying the price of a pay-per-use product	POST /v2/bills/ratings/on-demand-resources	billing:contract:viewDiscount	Grants the permission to view discount and price information.
		Querying the price of a yearly/monthly product	POST /v2/bills/ratings/period-resources/subscribe-rate	billing:contract:viewDiscount	Grants the permission to view discount and price information.
		Querying the renewal price of yearly/monthly resources	POST /v2/bills/ratings/period-resources/renew-rate	billing:contract:viewDiscount	Grants the permission to view discount and price information.
Managing accounts	Managing accounts	Querying the Account Balance	GET /v2/accounts/customer-accounts/balances	billing:balance:view	Grants the permission to view account information.
Managing transactions	Managing coupons	Querying coupons	GET /v2/promotions/benefits/coupons	billing:coupon:view	Grants the permission to view discount coupons, flexi-purchase coupons, and cash coupons.
	Managing yearly/monthly orders	Querying orders	GET /v2/orders/customer-orders	billing:order:view	Grants the permission to view order information.

Scenario	Sub-Scenario	API	API URL	Action	Action Description
		Grants the permission to querying order details.	GET /v2/orders/customer-orders/details/{order_id}	billing:order:view	Grants the permission to view order information.
		Paying for Yearly/Monthly Orders	POST /v2/orders/customer-orders/pay	billing:order:pay	Grants the permission to pay for orders.
		Querying Available Discounts for Orders	GET /v2/orders/customer-orders/order-discounts	billing:contract:viewDiscount	Grants the permission to view discount and price information.
		Paying for Yearly/Monthly Orders	POST /v3/orders/customer-orders/pay	billing:order:pay	Grants the permission to pay for orders.
		Querying Refund Order Amount	GET /v2/orders/customer-orders/refund-orders	billing:order:view	Grants the permission to view order information.
	Managing yearly/monthly resources	Querying Yearly/monthly Resources	POST /v2/orders/suscriptions/resources/query	• billing:subscription:view • billing:order:view (to be brought offline)	Grants the permission to view order information.

Scenario	Sub-Scenario	API	API URL	Action	Action Description
		Renewing subscriptions to yearly/monthly resources	POST /v2/orders/subscriptions/resources/renew	billing:subscription:renew	Grants the permission to place orders, cancel orders, and modify recipient information.
		Unsubscribing from yearly/monthly resources	POST /v2/orders/subscriptions/resources/unsubscribe	billing:subscription:unsubscribe	Grants the permission to place orders, cancel orders, and modify recipient information. For details, see en-us_topic_0000001844443526.xml.
		Enabling automatic renewal for yearly/monthly resources	POST /v2/orders/subscriptions/resources/autorenew/**	billing:subscription:renew	Grants the permission to 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	Grants the permission to place orders, cancel orders, and modify recipient information.

Scenario	Sub-Scenario	API	API URL	Action	Action Description
		Enabling/Canceling the Change from Yearly/Monthly Subscriptions to Pay-Per-Use upon Expiration.	POST /v2/orders/subscriptions/resources/to-on-demand	billing:subscription:renew	Grants the permission to place orders, cancel orders, and modify recipient information.
	Managing resource packages	Querying resource packages	POST /v3/payments/free-resources/query	billing:resourcePackages:view	Grants the permission to view bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends.
		Querying Resource Package Usage Details	GET /v2/bills/customer-bills/free-resources-usage-records	• billing:resourcePackages:view • billing:billDetail:view (to be brought offline)	Grants the permission to view expenditure details, resource expenditures, bill analysis, and historical payments.

Scenario	Sub-Scenario	API	API URL	Action	Action Description
		Querying resource package usage	POST /v2/payments/free-resources/usages/details/query	billing:resourcePackages:view	Grants the permission to 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	Grants the permission to view expenditure details, resource expenditures, bill analysis, and historical payments.
		Querying bill summary	GET /v2/bills/customer-bills/monthly-sum	billing:bill:view	Grants the permission to view bills, monthly costs, usage details, cost management, expenditures and revenues, and cost trends.

Scenario	Sub-Scenario	API	API URL	Action	Action Description
		Querying expenditure records	GET /v2/bills/customer-bills/res-fee-records	• billing:billDetail:view • billing:bill:view (to be brought offline)	Grants the permission to 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	Grants the permission to view cost analysis.
Managing an enterprise	Managing enterprise projects	Enabling the enterprise project management service	POST /v2/enterprises/enterprise-projects/authority	Billing::activeEPFinance	Grants permissions to enable the enterprise project function.
	Managing enterprise accounts	Querying enterprise member accounts	GET /v2/enterprises/multi-accounts/sub-customers	businessUnitCenter:businessUnit:view	Grants the permission to view organizations and accounts in Enterprise Center.
Managing invoices	Managing invoices	Querying Invoices	GET /v1.0/{domain_id}/payments/intl-invoices	billing:invoice:manage	Grants the permission to request invoices and view invoice information.

Resources

BSS does not support resource-specific permission control through SCPs. To allow access to BSS, use the wildcard (*) in the **Resource** element in an SCP, and this SCP will apply to all resources of BSS.

Conditions

BSS does not support service-specific condition keys in SCPs. You can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.15 Migration

5.10.15.1 Object Storage Migration Service (OMS)

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 topic 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 OMS, 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 OMS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for OMS.

Table 5-266 Actions supported by OMS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
oms:task:list	Grants permission to list migration tasks.	list	task	-
oms:task:create	Grants permission to create a migration task.	write	task	-
oms:task:get	Grants permission to query details about a migration task.	read	task	-
oms:task:delete	Grants permission to delete a migration task.	write	task	-
oms:task:update	Grants permission to update a migration task.	write	task	-
oms:synctask:list	Grants permission to list synchronization tasks.	list	synctask	-
oms:synctask:create	Grants permission to create a synchronization task.	write	synctask	-
oms:synctask:get	Grants permission to query details about a synchronization task.	read	synctask	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
oms:synctask:delete	Grants permission to delete a synchronization task.	write	synctask	-
oms:synctask:statistics	Grants permission to query statistics about a synchronization task.	read	synctask	-
oms:synctask:update	Grants permission to update a synchronization task.	write	synctask	-
oms:synctask:createEvent	Grants permission to create a synchronization event.	write	synctask	-
oms:taskgroup:create	Grants permission to create a migration task group.	write	taskgroup	-
oms:taskgroup:list	Grants permission to list migration task groups.	list	taskgroup	-
oms:taskgroup:get	Grants permission to query details about a migration task group.	read	taskgroup	-
oms:taskgroup:delete	Grants permission to delete a migration task group.	write	taskgroup	-
oms:taskgroup:update	Grants permission to update a migration task group.	write	taskgroup	-
oms::listObjects	Grants permission to list objects in a bucket.	list	-	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
oms::checkCdnInfo	Grants permission to check the connectivity between a bucket and CDN.	read	-	-
oms::listBuckets	Grants permission to list buckets.	list	-	-
oms::listBucketRegions	Grants permission to query the region of a bucket.	list	-	-
oms::checkBucketPrefix	Grants permission to check whether a bucket has objects with a specified prefix.	read	-	-
oms::listCloudRegions	Grants permission to query regions supported for a cloud vendor.	list	-	-
oms::listCloudTypes	Grants permission to list supported cloud vendors.	list	-	-

Each API of OMS usually supports one or more actions. **Table 5-267** lists the supported actions and dependencies.

Table 5-267 Actions and dependencies supported by OMS APIs

API	Action	Dependencies
GET /v2/{project_id}/tasks	oms:task:list	-
POST /v2/{project_id}/tasks	oms:task:create	-
GET /v2/{project_id}/tasks/{task_id}	oms:task:get	-
DELETE /v2/{project_id}/tasks/{task_id}	oms:task:delete	-
POST /v2/{project_id}/tasks/{task_id}/stop	oms:task:update	-
POST /v2/{project_id}/tasks/{task_id}/start	oms:task:update	-

API	Action	Dependencies
PUT /v2/{project_id}/tasks/{task_id}/bandwidth-policy	oms:task:update	-
PUT /v2/{project_id}/tasks/{task_id}/access-keys	oms:task:update	-
GET /v2/{project_id}/sync-tasks	oms:synctask:list	-
POST /v2/{project_id}/sync-tasks	oms:synctask:create	-
GET /v2/{project_id}/sync-tasks/{sync_task_id}	oms:synctask:get	-
DELETE /v2/{project_id}/sync-tasks/{sync_task_id}	oms:synctask:delete	-
GET /v2/{project_id}/sync-tasks/{sync_task_id}/statistics	oms:synctask:statistics	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/stop	oms:synctask:update	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/start	oms:synctask:update	-
POST /v2/{project_id}/sync-tasks/{sync_task_id}/events	oms:synctask:createEvent	-
POST /v2/{project_id}/taskgroups	oms:taskgroup:create	-
GET /v2/{project_id}/taskgroups	oms:taskgroup:list	-
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	-

API	Action	Dependencies
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 SCP policy applies to. If you specify a resource type for any action in **Table 5-268**, 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 OMS.

Table 5-268 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 an SCP.

It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

5.10.15.2 Server Migration Service (SMS)

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 topic 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 identity policy 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 SMS, 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 SMS, see **Conditions**.

The following table lists the actions that you can define in SCP statements for SMS.

Table 5-269 Actions supported by SMS

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sms:template:list	Grants permission to list templates.	list	template	-
sms:template:create	Grants permission to create a template.	write	template	-
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:template:update	Grants permission to modify a template.	write	template	-
sms:template:getTargetPassword	Grants permission to query the target server password in a template.	read	template	-
sms:template:delete	Grants permission to delete a template.	write	template	-
sms:server:listErrors	Grants permission to list failed source servers.	list	server	-
sms:server:list	Grants permission to list source servers.	list	server	g:EnterpriseProjectId
sms:server:register	Grants permission to register a source server with SMS.	write	server	g:EnterpriseProjectId
sms:server:batchDelete	Grants permission to batch delete source server records.	write	server	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sms:server:get	Grants permission to query the details about a source server.	read	server	g:EnterpriseProjectId
sms:server:update	Grants permission to modify a source server name.	write	server	g:EnterpriseProjectId
sms:server:delete	Grants permission to delete a source server record.	write	server	g:EnterpriseProjectId
sms:server:updateDiskInfo	Grants permission to update disk information.	write	server	g:EnterpriseProjectId
sms:server:overview	Grants permission to obtain the summary of source servers.	read	server	-
sms:server:updateState	Grants permission to update the migration task status for a source server.	write	server	g:EnterpriseProjectId
sms:server:listTask	Grants permission to list migration tasks.	list	server	g:EnterpriseProjectId
sms:server:createTask	Grants permission to create a migration task.	write	server	g:EnterpriseProjectId
sms:server:batchDeleteTask	Grants permission to batch delete migration tasks.	write	server	g:EnterpriseProjectId
sms:server:getTask	Grants permission to query the details about a migration task.	read	server	g:EnterpriseProjectId
sms:server:updateTask	Grants permission to update a migration task.	write	server	g:EnterpriseProjectId
sms:server:deleteTask	Grants permission to delete a migration task.	write	server	g:EnterpriseProjectId

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sms:server:manageTask	Grants permission to manage migration tasks.	write	server	g:EnterpriseProjectId
sms:server:updateTaskProgress	Grants permission to report the migration progress and rate.	write	server	g:EnterpriseProjectId
sms:server:unlock	Grants permission to unlock a target server.	write	server	g:EnterpriseProjectId
sms:server:collectLog	Grants permission to upload migration task logs.	write	server	g:EnterpriseProjectId
sms:server:getTaskPassphrase	Grants permission to query a certificate passphrase.	read	server	g:EnterpriseProjectId
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	g:EnterpriseProjectId
sms:server:updateTaskSpeedLimit	Grants permission to set traffic limiting rules for a migration task.	write	server	g:EnterpriseProjectId
sms:server:getCommand	Grants permission to obtain commands from SMS.	read	server	g:EnterpriseProjectId
sms:server:updateCommandResult	Grants permission to report command execution results to SMS.	write	server	g:EnterpriseProjectId
sms:server:getCert	Grants permission to obtain an SSL certificate and private key.	read	server	g:EnterpriseProjectId
sms:migproject:list	Grants permission to list migration projects.	list	migproject	-

Action	Description	Access Level	Resource Type (*: required)	Condition Key
sms:migproject:create	Grants permission to create a migration project.	write	migproject	-
sms:migproject:get	Grants permission to query details about a migration project.	read	migproject	-
sms:migproject:update	Grants permission to update a migration project.	write	migproject	-
sms:migproject:delete	Grants permission to delete a migration project.	write	migproject	-
sms:migproject:update	Grants permission to change the default migration project.	write	migproject	-
sms::getConfig	Grants permission to obtain Agent configuration information.	read	-	-
sms:server:updateNetworkCheckInfo	Grants permission to update network measurement information.	write	task	g:EnterpriseProjectId
sms:server:getTaskConfig	Grants permission to query the settings of advanced migration options of a task.	read	task	g:EnterpriseProjectId
sms:server:updateTaskConfig	Grants permission to set advanced migration options for a task.	write	task	g:EnterpriseProjectId

Each API of SMS usually supports one or more actions. **Table 5-270** lists the supported actions and dependencies.

Table 5-270 Actions and dependencies supported by SMS APIs

API	Action	Dependencies
GET /v3/vm/templates	sms:template:list	-

API	Action	Dependencies
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	-
POST /v3/sources/delete	sms:server:batchDelete	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
GET /v3/sources/{source_id}	sms:server:get	-
PUT /v3/sources/{source_id}	sms:server:update	-

API	Action	Dependencies
DELETE /v3/sources/{source_id}	sms:server:delete	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
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	-
POST /v3/tasks/delete	sms:server:batchDeleteTask	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
GET /v3/tasks/{task_id}	sms:server:getTask	-
PUT /v3/tasks/{task_id}	sms:server:updateTask	-

API	Action	Dependencies
DELETE /v3/tasks/{task_id}	sms:server:deleteTask	• ecs:cloudServers:showServer • ecs:cloudServers:attach • evs:volumes:use • ecs:cloudServers:stop • ecs:cloudServers:start • ecs:cloudServers:detachVolume • evs:volumes:delete • evs:snapshots:delete • evs:volumes:get
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	-
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	-

API	Action	Dependencies
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 SCP applies to. If you specify a resource type for any action in **Table 5-271**, 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 specify in SCP statements for SMS.

Table 5-271 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 an SCP.

It can only use global condition keys applicable to all services. For details, see Global Condition Keys.

6 Managing Tag Policies

6.1 Overview of a Tag Policy

Introduction

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. In a tag policy, you specify tagging rules applicable to resources when they are tagged. Untagged resources and tags that are not defined in the tag policy are not evaluated for compliance with the tag policy.

For example, a tag policy can specify that a tag attached to a resource must use the case treatment and tag values defined in the tag policy. If the case and value of the tag do not comply with the tag policy, the resource will be marked as non-compliant.

Currently, tag policies can be used as preventive governance policies. Specifically, if enforcement is enabled for a tag policy, non-compliant tagging operations will be prevented from being performed on specified resource types.

You can attach tag policies to the root OU, other OUs, and accounts within your organization. When you attach a tag policy to the root OU and other OUs, all their child OUs and member accounts inherit that tag policy. The effective tag policy for an account specifies the tagging rules that apply to the account. It is the combination of tag policies that account inherits and tag policies directly attached to that account.

Functions

Managing tag policies

You can create, update, delete, attach, or detach tag policies. OUs and accounts inherit tag policies from one or more of their parent nodes (such as parent OUs). The inherited tag policies are aggregated with those directly attached to the OUs and accounts to form the effective tag policy.

6.2 Tag Policy Syntax

Basic Syntax

The following tag policy shows basic tag policy syntax:

```
{
   "tags": {
      "costcenter": {               <!-- policy key -->
         "tag_key": {
            "@@assign": "CostCenter"               <!-- tag key -->
         },
         "tag_value": {
            "@@assign": [
               "100",               <!-- policy value -->
               "200"
            ]
         },
         "enforced_for": {               <!-- enforcement -->
            "@@assign": [
               "apig:instance"               <!-- service or resource type -->
            ]
         }
      }
   }
}
```

- Policy key: A policy key uniquely identifies a policy statement. It must match the value for the tag key, except for the case treatment.
- Tag key: The value for the tag key must match the value for the policy key. But since the policy key value is case insensitive, the capitalization can be different. If the tag key is not defined, lowercase is the default case treatment for tag keys. In this example, **costcenter** is the policy key and **CostCenter** is the tag key, and **CostCenter** is the case treatment that is required for compliance with the tag policy. If the policy key is set to **CostCenter** and the tag key is not defined, the lowercase **costcenter** will be the case treatment required for tag compliance evaluation.
- Policy value: A list of one or more acceptable tag values for the tag key. If you do not specify tag values for a tag key, any value (including no value at all) is considered compliant.
- Enforcement: An **enforced_for** field indicates whether to prevent any non-compliant tagging operations on specified services and resources. If you do not specify any services or resource types in a tag policy, the tag policy will not apply to any resources.
- Wildcard: You can use the wildcard (*) in tag values and the **enforced_for** field provided that you adhere to the following rules:
  - You can use only one wildcard for each tag value. For example, ***@example.com** is allowed, but ***@*.com** is not.
  - For the **enforced_for** field, you can use **<service>:*** to enable enforcement for all resources for a service, but you cannot use a wildcard to specify all services or specify a resource of all services.

Inheritance Operators

In the preceding example tag policy, the operator @@assign used in the tag key, tag value, and enforcement is an inheritance operator.

Inheritance operators specify how directly attached tag policies and inherited tag policies are merged into the account's effective tag policy. Such operators include value-setting operators and child control operators.

- **Value-setting operators**

  You can use the following value-setting operators to control how your policy interacts with its parent policies.

  Table 6-1 Value-setting operators

Operator	Description
@@assign	Overwrites any inherited policy settings with the specified setting. If the specified setting is not inherited, this operator adds it to the effective tag policy. This operator can apply to any policy setting of any type. For single-valued settings, this operator replaces the inherited value with the specified value. For multi-valued settings (JSON arrays), this operator removes all inherited values and replaces them with the values specified for this policy.
@@append	Adds the specified settings to the inherited settings, without deleting any settings. If the specified setting is not inherited, this operator adds it to the effective tag policy. You can only use this operator with multi-valued settings. This operator adds the specified value to any values in the inherited array.
@@remove	Removes the specified inherited setting (if there is one) from the effective policy. You can only use this operator with multi-valued settings. This operator removes only the specified values from the array of values inherited from the parent policies. Other values can be retained in the array and inherited by child policies.

- **Child control operators**

  Child control operators specify which value-setting operators child OUs and accounts can use in child policies. By default, all operators (@@all) are allowed.

  - "@@operators_allowed_for_child_policies":["@@all"] indicates that child OUs and accounts can use any operator in policies. By default, all operators are allowed in child policies.
  - "@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"] indicates that child OUs and accounts can use only the

specified operators in child policies. You can specify one or more value-setting operators in this child control operator.

- "@@operators_allowed_for_child_policies":["@@none"] indicates that child OUs and accounts cannot use operators in policies. You can use this operator to effectively lock the values defined in a parent policy so that the child policies cannot add, append, or delete those values.

6.3 Enabling or Disabling the Tag Policy Type

You can enable or disable the tag policy type from the organization' management account, but not from any delegated administrator.

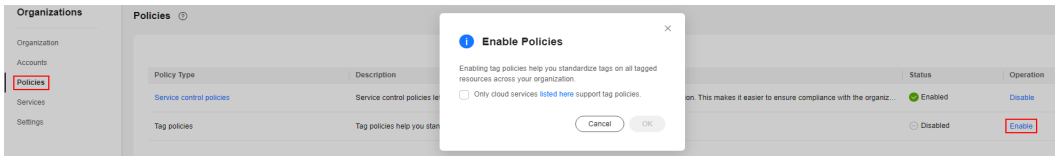
Enabling the Tag Policy Type

Before you can create and attach tag policies to the OUs and accounts in your organization, you must enable the tag policy type. The only way to enable the tag policy type is by using the organization's management account.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Enable** in the **Operation** column of tag policies.

Figure 6-1 Enabling the tag policy type



Step 3 In the displayed dialog box, select the check box and click **OK**.

----End

Disabling the Tag Policy Type

If you no longer want to use tag policies in your organization, you can disable the tag policy type only from the organization's management account.

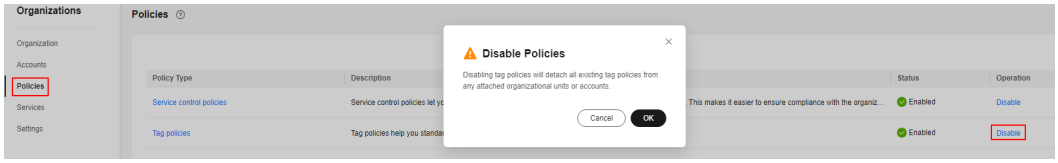
CAUTION

- After the tag policy type is disabled in an organization, all tag policies are automatically detached from all OUs and accounts in the organization. However, the policies are not deleted.
- If you disable the tag policy type, attachments of tag policies to entities will be lost. If you later re-enable the tag policy type, you must use the management account to re-attach tag policies to the entities.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Disable** in the **Operation** column of tag policies.

Figure 6-2 Disabling the tag policy type



Step 3 Click **OK** in the displayed dialog box.

----End

6.4 Creating a Tag Policy

To standardize the usage of tags in your organization, you can create a tag policy to formulate tag rules.

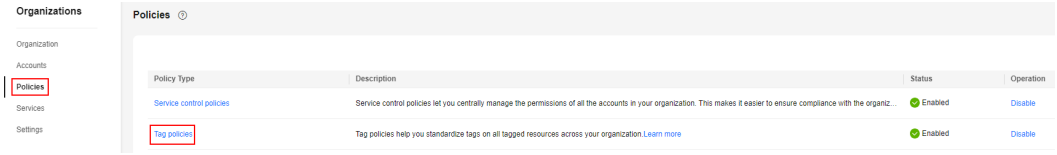
You can create a tag policy from the organization administrator, but not from any delegated administrator.

Procedure

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 Access the **Policies** page, and click **Tag policies**.

Figure 6-3 Accessing the **Tag policies** page



Step 3 Click **Create Policy**.

Step 4 Edit the policy name. The policy name is automatically generated when you create a policy, but you can change the policy name if needed. Ensure that you are entering a unique policy name. It must be different from any other existing policy.

(Optional) You can also enter a description for the policy.

Step 5 Edit the policy content. Currently, you can edit the policy content using the visual editor or JSON.

- Visual editor: When you use the visual editor to edit a policy, you do not need to understand the JSON syntax. After you edit in the visual editor, the new policy is generated automatically. The procedure is as follows:
  a. Enter the key for the tag you want to define in the tag policy.
  b. Use the capitalization you specified above for the tag key.

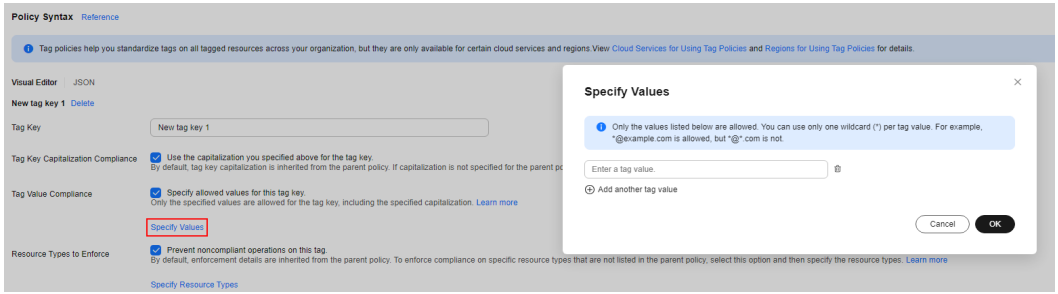
     If you select this option, the capitalization you specified for **Tag Key** is used for checking compliance. If you do not select this option, tag keys in all lowercase characters are considered compliant even if **Tag Key**

contains uppercase characters. For example, when you enter **CostCenter** for **Tag Key**, if you select this option, **CostCenter** will be the standard for compliance check; if you do not select this option, **costcenter** will be the standard.

c. Specify allowed values for this tag key.

If you select this option and click **Specify Values** to specify one or more allowed values for the tag key, only those values you specified are considered compliant. If you do not select this option or you select this option but do not specify any values, any value (including no value at all) is considered compliant.

Figure 6-4 Specifying allowed values for this tag key



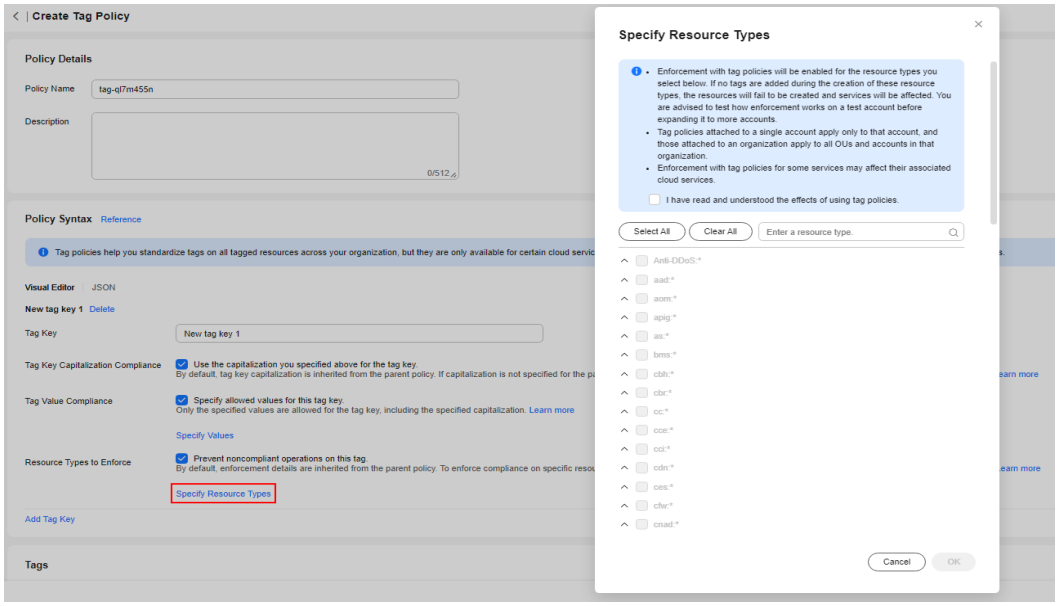
d. Specify resource types to enforce the tag policy.

Select the **Prevent noncompliant operations on this tag.** option and click **Specify Resource Types**. In the displayed dialog box, read and confirm the effects of using tag policies. Then, select resource types and click **OK**.

NOTE

If you do not specify any services or resource types, the tag policy will not apply to any resources.

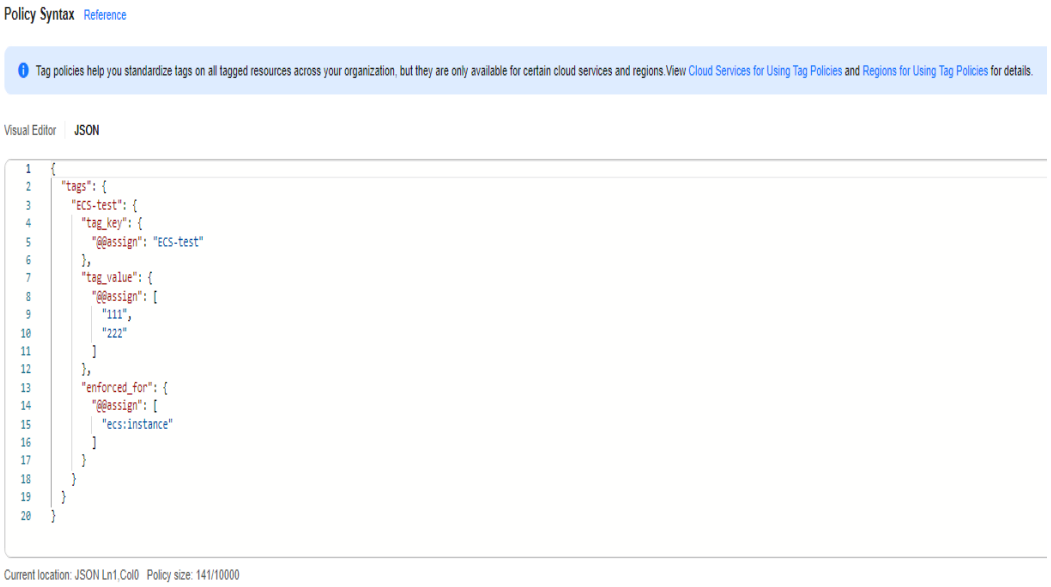
Figure 6-5 Specifying resource types



e. Click **Add Tag Key** to add another tag key to this tag policy.

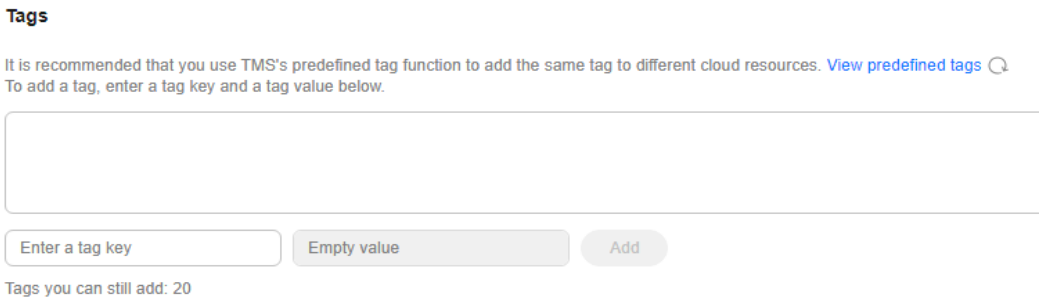
- JSON: When using JSON syntax, you can edit the policy text by referring to **Tag Policy Syntax**. The system automatically verifies the syntax. If the syntax is incorrect, modify it as prompted.

Figure 6-6 Editing a policy using JSON



Step 6 (Optional) Add one or more tags. Enter a tag key and a tag value, and click **Add**.

Figure 6-7 Adding a tag



Step 7 Click **Save** in the lower right corner. If the tag policy is created successfully, it will be added to the list.

----End

6.5 Viewing the Effective Tag Policy

You can attach tag policies to the root OU, other OUs, and accounts within your organization. When you attach a tag policy to the root OU and other OUs, all their child OUs and member accounts inherit that tag policy. The effective tag policy for an account specifies the tagging rules that apply to the account. It is the combination of tag policies that account inherits and tag policies directly attached to that account.

The following describes how a tag policy is prioritized as the effective tag policy:

- Tag policies attached to entities at the same hierarchy level:
  - Single-valued operators: If you attach multiple tag policies, the first policy using the @@assign operator will be considered to be the effective tag policy.
  - Multi-valued operators: If you attach multiple tag policies, the first policy using the @@assign operator will be considered to be the effective tag policy, and the @@append and @@remove operators used by other policies still take effect.
- Tag policies attached to entities at the different hierarchy levels:

  If the upper- and lower-level entities use the same tag key, tag policies are calculated from the upper-level entities to the lower-level entities based on the types of child control operators to comprise the effective tag policy. If the upper and lower levels use different tag keys, the combination of their tag policies comprises the effective tag policy.

To view the effective tag policy for the root OU, other OUs, and accounts of an organization on the management console, use the following procedure:

Procedure

Step 1 Log in to the Organizations console on Huawei Cloud and access the **Organization** page.

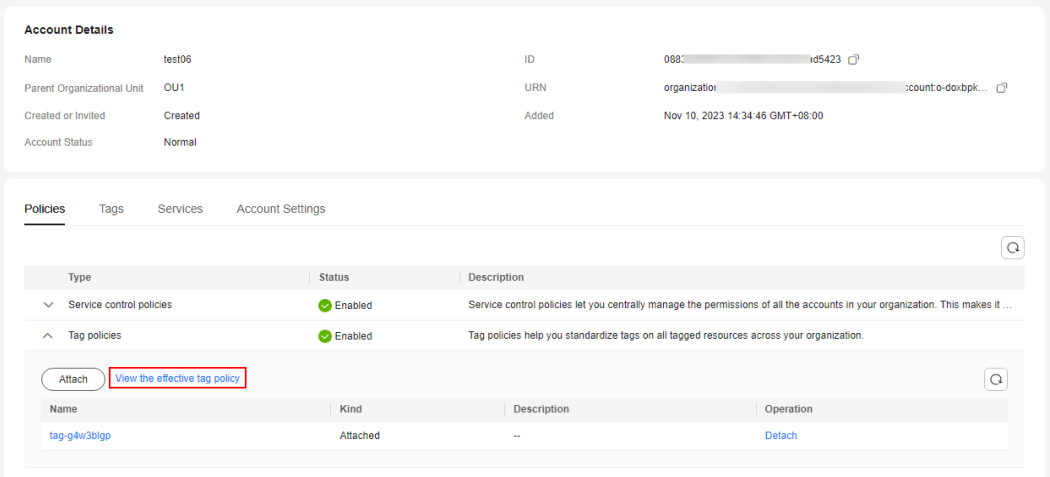
Step 2 Choose **Organization** in the navigation pane.

Step 3 Click the root OU, specific OU, or account of your organization. You can view its details on the right of the organization tree.

Step 4 Click the **Policies** tab.

Step 5 Expand the tag policy list and click **View the effective tag policy** above the list. The effective tag policy is presented in JSON.

Figure 6-8 Viewing the effective tag policy



----End

6.6 Editing or Deleting a Tag Policy

The following describes how to edit and delete a tag policy.

You can edit or delete a tag policy from the organization administrator, but not from a delegated administrator.

Editing a Tag Policy

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 Access the **Policies** page, and click **Tag policies**.

Step 3 Locate the target tag policy and click **Modify** in the **Operation** column. The **Edit Tag Policy** page is displayed.

Figure 6-9 Editing a tag policy

Step 4 Enter a new policy name and description.

Step 5 Edit the policy content if needed. You can choose either visual editor or JSON to edit the policy.

Step 6 Click **Save** in the lower right corner. If the tag policy is updated successfully, it will be added to the list.

----End

Deleting a Tag Policy

A tag policy that is attached to OUs or accounts cannot be deleted. To delete such a tag policy, you need to detach it from the OUs or accounts first.

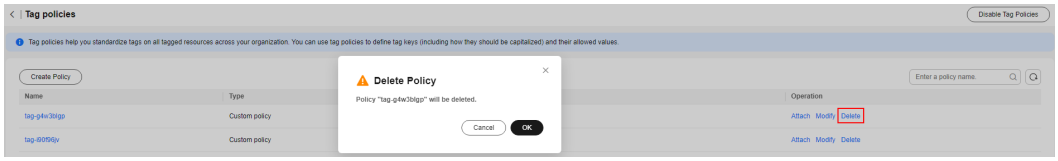
Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 Access the **Policies** page, and click **Tag policies**.

Step 3 Locate the tag policy you want to delete and click **Delete** in the **Operation** column.

Step 4 Click **OK** in the displayed dialog box.

Figure 6-10 Deleting a tag policy



----End

6.7 Attaching or Detaching a Tag Policy

You can attach a tag policy to or detach it from the root OU, other OUs or accounts from the organization's management account.

Constraints

- You can attach up to 10 tag policies to an account.
- You can attach or detach a tag policy from only the organization administrator, but not from a delegated administrator.
- Tag policies are applied within 30 minutes after they are attached.

Attaching a Tag Policy

Method 1:

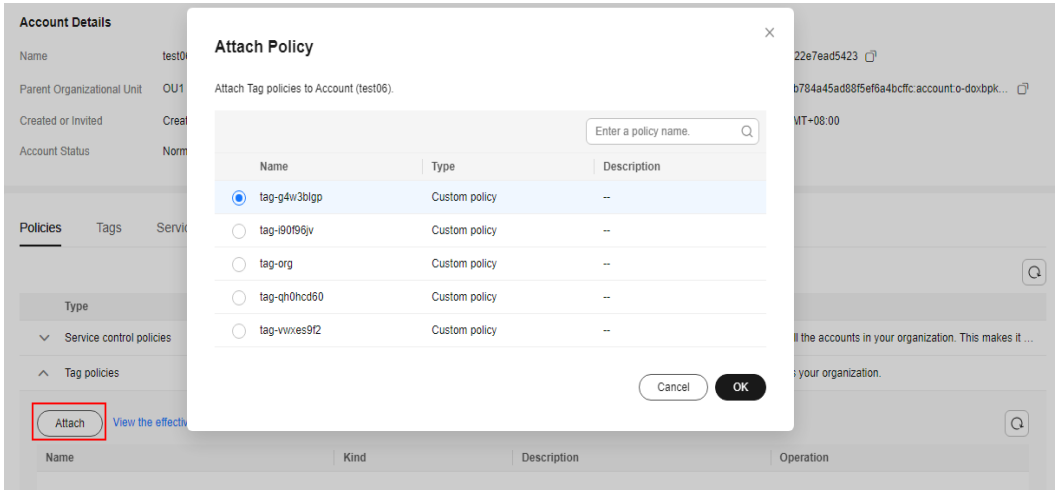
Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU or account you want to attach a tag policy to.

Step 3 On the details page, click the **Policies** tab. On the page, expand **Tag policies** and click **Attach**.

Step 4 Select the tag policy you want to attach and click **OK**.

Figure 6-11 Attaching a tag policy



----End

Method 2:

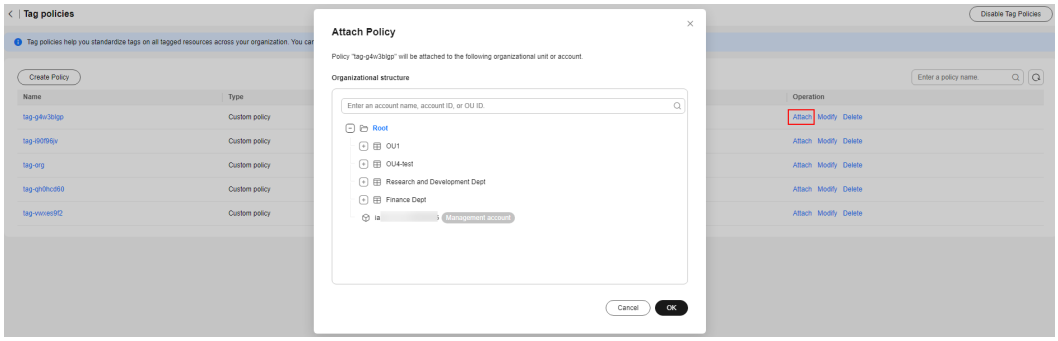
Step 1 Access the **Policies** page on the Organizations console.

Step 2 Click **Tag policies**. The list of tag policies is displayed.

Step 3 Locate the tag policy you want to attach and click **Attach** in the **Operation** column. Then, select the OU or account you want to attach the policy to.

Step 4 Click **OK**.

Figure 6-12 Attaching a tag policy



----End

Detaching a Tag Policy

Method 1:

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU or account you want to detach a tag policy from.

Step 3 On the details page, click the **Policies** tab. On the page, expand **Tag policies**, locate the target tag policy and click **Detach** in the **Operation** column.

Figure 6-13 Detaching a tag policy

Step 4 Click **Detach** in the displayed dialog box.

----End

Method 2:

Step 1 Access the **Policies** page on the Organizations console.

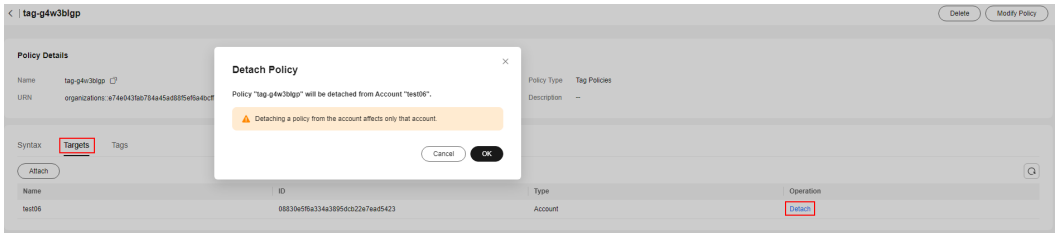
Step 2 Click **Tag policies**. The list of tag policies is displayed.

Step 3 Click the name of the target tag policy and click the **Targets** tab.

Step 4 Locate the OU or account that you want to detach the tag policy from and click **Detach** in the **Operation** column.

Step 5 Click **OK**.

Figure 6-14 Detaching a tag policy



----End

6.8 Cloud Services for Using Tag Policies

Tag policies are available for the following cloud services and resource types:

Table 6-2 Supported cloud services and resources types

Service Name	Resource Type
Cloud Native Anti-DDoS Basic	Public IP addresses
Anti-DDoS Service	Instances
Application Operations Management (AOM)	Alarm rules
API Gateway	Instances
Auto Scaling (AS)	Scaling groups
Bare Metal Server (BMS)	Instances
Cloud Bastion Host (CBH)	Instances
Cloud Backup and Recovery (CBR)	Vaults
Cloud Connect	• Bandwidth packages • Central network • Cloud connections
Cloud Container Engine (CCE)	Clusters
Cloud Container Instance (CCI)	Namespace
Content Delivery Network (CDN)	Domain

Service Name	Resource Type
Cloud Eye	Alarm rules
Cloud Firewall (CFW)	Instances
Cloud Native Anti-DDoS Advanced (CNAD)	Packages
Cloud Service Engine (CSE)	Engine
Cloud Secret Management Service (CSMS)	Secret
Cloud Search Service (CSS)	• Clusters • Log stream • Repository
Cloud Trace Service (CTS)	Trackers
DataArts Studio	• Instances • Workspace
Database Security Service (DBSS)	Audit instances
Direct Connect (DCAAS)	• Direct connections • Global DC gateways (gdgw) • Lag • Virtual gateways • Virtual interfaces
Distributed Cache Service (DCS)	Instances
Document Database Service (DDS)	Instance names
Dedicated Hardware Security Module (Dedicated HSM)	Hardware security modules
Data Lake Insight (DLI)	• Databases • Enhanced datasource connections • Elastic resource pools • Jobs • Queues • Resources
Distributed Message Service (DMS)	• Kafka instances • RabbitMQ instances • RocketMQ instances
Domain Name Service (DNS)	• PTR • Domain names
Data Replication Service (DRS)	Jobs

Service Name	Resource Type
Data Warehouse Service (DWS)	Clusters
Elastic Cloud Server (ECS)	Instances
Elastic Load Balance (ELB)	• Listeners • Load balancers
Enterprise Router	• Attachments • Instances • Route tables
Elastic Volume Service (EVS)	Volume
FunctionGraph	Functions
Global Accelerator (GA)	• Accelerators • Listeners
GaussDB	Instances
GaussDB(for MySQL)	Instances
GeminiDB (originally named GaussDB for NoSQL)	Instances
Identity and Access Management (IAM)	• Agencies • Users
Image Management Service (IMS)	Images
IoT Device Access (IoTDA)	Instances
Key Management Service (KMS)	Customer master keys
Log Tank Service (LTS)	• Log access configuration • Host groups • Log groups • Log stream
ModelArts	• Notebook • Resource pools • Services • Training jobs
MapReduce Service (MRS)	Clusters
NAT Gateway	• Public gateways • Private gateways • Private transit IP addresses • Transit subnets

Service Name	Resource Type
Organizations	• Accounts • Organizational units • Policies • Root
Private Certificate Authority (PCA)	Private CA
Resource Access Manager (RAM)	Resource shares
Relational Database Service (RDS)	Instances
Config (original service name: RMS)	Policy assignments
SSL Certificate Manager (SCM)	Certificates
SecMaster	Workspace
ServiceStage	• Applications • Environment
Scalable File Service Turbo (SFS Turbo)	SFS Turbo (shares)
Simple Message Notification (SMN)	Topics
Virtual Private Cloud (VPC)	• Public IP addresses • Subnets • VPC
VPC Endpoint (VPCEP)	• Endpoint services • Endpoints
Virtual Private Network (VPN)	• Peer gateways • VPN connections • VPN gateways
Web Application Firewall (WAF)	Premium instances

6.9 Regions for Using Tag Policies

Tag policies are available in the following regions:

Table 6-3 Supported regions

Region Name	Region Code
AP-Singapore	ap-southeast-3
AP-Bangkok	ap-southeast-2
AP-Jakarta	ap-southeast-4

Region Name	Region Code
CN East-Shanghai1	cn-east-3
CN East-Shanghai2	cn-east-2
CN-Hong Kong	ap-southeast-1
CN North-Beijing1	cn-north-1
CN North-Beijing4	cn-north-4
CN South-Guangzhou	cn-south-1
CN North-Ulanqab1	cn-north-9
CN Southwest-Guiyang1	cn-southwest-2
CN East-Qingdao	cn-east-5
TR-Istanbul	tr-west-1
AF-Johannesburg	af-south-1
LA-Mexico City1	na-mexico-1
LA-Mexico City2	la-north-2
LA-Sao Paulo1	sa-brazil-1
LA-Santiago	la-south-2
ME-Riyadh	me-east-1

7 Managing Trusted Services

7.1 Overview of a Trusted Service

What Is a Trusted Service?

You can use the management account in Organizations to enable trusted access for a supported Huawei Cloud service, called a trusted service. A trusted service can perform tasks in your organization on your behalf. Each trusted service has access to the information about the OUs and member accounts in your organization and also can manage the entire organization. For example, if you enable CTS as a trusted service for Organizations, CTS can obtain information about OUs and member accounts to record the operations in all accounts within the organization. For cloud services that can be enabled with trusted access, see **Trusted Services for Organizations**.

Delegated Administrator

A delegated administrator account is a member account that has special permissions in an organization. The management account of your organization can designate a member account to be a delegated administrator account for a trusted service. All the users in the delegated administrator account will have organizational management capabilities. For example, if a member account becomes the delegated administrator of CTS, the account can view the CTS logs of all member accounts in the organization.

Service-linked Agency

Organizations uses IAM trust agencies to enable trusted services to perform tasks on your behalf in your organization's member accounts. When you enable a trusted service, the service can request that Organizations create a service-linked agency in its member accounts. The trusted service does this asynchronously, as needed. The service-linked agency has predefined IAM permissions that allow the trusted service to perform specific tasks within that account. This means that the capabilities of that cloud service are extended to the entire multi-account organization. For details about the supported trusted services and their functions, see **Trusted Services for Organizations**.

When you create an account in your organization or invite an existing account to join your organization, Organizations provisions the member account with a service-linked agency with the system-defined permission OrganizationsServiceLinkedAgencyPolicy, which is applicable to all resources. Only the Organizations service itself can assume this agency. This agency has permission that allows Organizations to create service-linked agencies for other cloud services.

NOTE

Organizations SCPs do not affect service-linked agencies, and operations performed using service-linked agencies are not restricted by SCPs.

7.2 Enabling or Disabling a Trusted Service

- If the organization administrator disables trusted access for a cloud service, the service can no longer create a service-linked agency in the member accounts.
- If the organization administrator closes the organization or a member account leaves the organization, Organizations will clear its service-linked agency.
- Before disabling trusted access for the AOM service, delete multi-account instances on the AOM console and then disable the trusted access on the Organizations console. Otherwise, the multi-account instances will continue retrieving the member accounts' metric data.
- Before disabling trusted access for the LTS service, delete the configurations of multi-account log aggregation on the LTS console and then disable the trusted access on the Organizations console. Otherwise, the multi-account log aggregation will continue retrieving the member accounts' logs.

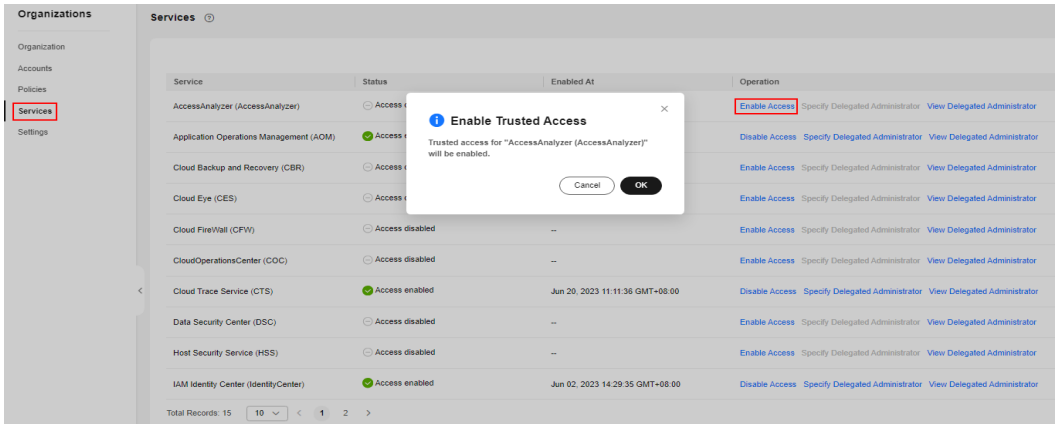
Enabling a Trusted Service

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Services** page, locate the target trusted service and click **Enable Access** in the **Operation** column.

Step 3 Click **OK** in the displayed dialog box.

Figure 7-1 Enabling a trusted service



----End

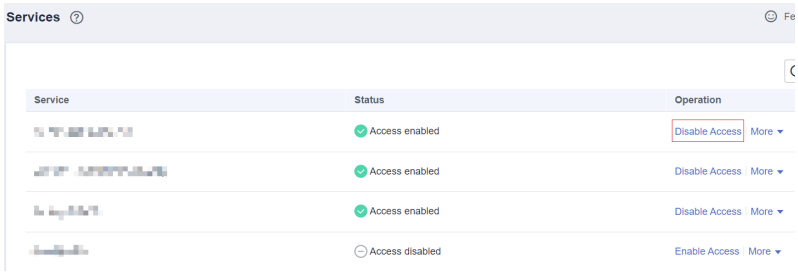
Disabling a Trusted Service

When logging in as the organization's management account, you can disable trusted services.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

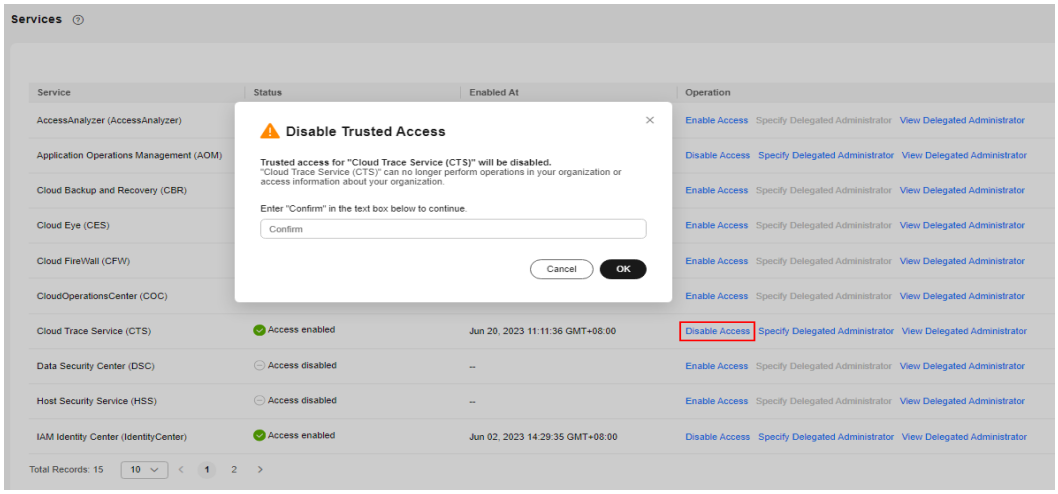
Step 2 On the **Services** page, locate the target trusted service and click **Disable Access** in the **Operation** column.

Figure 7-2 Disabling a trusted service



Step 3 In the displayed dialog box, enter "Confirm" and click **OK**.

Figure 7-3 Disabling a trusted service



----End

7.3 Trusted Services for Organizations

Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Services** page to view the trusted services for Organizations.

The following table lists the cloud services that can be used with Huawei Cloud Organizations.

Table 7-1 Trusted services for Organizations

Service Name	Benefits of Using with Organizations	Delegated Administrator	Reference
Config	You can create compliance rules, conformance packages, and resource aggregators for a given organization. The organization administrator or the delegated Config administrator can perform unified configurations, which will be applied to all normal member accounts in the organization.	Supported	• Organization Rules • Organization Conformance Packages • Resource Aggregation
Resource Access Manager (RAM)	You can easily share resources within a given organization. When your account is managed by an organization, you can share resources with all accounts in the organization. Accounts in the same organization can use the shared resources without being invited.	Supported	Enabling Sharing with Organizations

Service Name	Benefits of Using with Organizations	Delegated Administrator	Reference
Cloud Trace Service (CTS)	You can configure an organization tracker for a given organization. The organization administrator or delegated CTS administrator can apply the organization tracker to the entire organization for cloud audit, such as multi-account security audit.	Supported	Organization Trackers
Application Operations Management (AOM)	You can create Prometheus instances of the multi-account aggregation type. With this function enabled for a given organization, the organization administrator or delegated AOM administrator can centrally monitor the cloud service metrics across multiple member accounts in the organization.	Supported	Prometheus for Multi-Account Aggregation

Service Name	Benefits of Using with Organizations	Delegated Administrator	Reference
Cloud Backup and Recovery (CBR)	You can manage backup and replication policies for a given organization. The organization administrator or delegated CBR administrator can centrally create and configure organizational backup policies and replication policies for member accounts in the organization.	Supported	Organization Policy Management
Cloud Eye	You can view the dashboards across accounts in a given organization. The organization administrator or delegated Cloud Eye administrator can view the dashboards of all accounts in the organization.	Supported	Viewing Dashboards Across Accounts
Cloud Firewall (CFW)	You can securely and reliably aggregate data from and access resources across accounts. The organization administrator or delegated CFW administrator can protect the EIPs of all member accounts in the organization in a unified manner.	Supported	Multi-Account Management

Service Name	Benefits of Using with Organizations	Delegated Administrator	Reference
Data Security Center (DSC)	You can securely and reliably aggregate data from and access resources across accounts. The organization administrator and delegated DSC administrator can protect the data security of all member accounts in the organization, without login using each account.	Supported	Multi-Account Management
Host Security Service (HSS)	You can securely and reliably aggregate data from and access resources across accounts. The organization administrator or delegated HSS administrator can protect the workloads of all member accounts in the organization in a unified manner.	Supported	Account Management

Service Name	Benefits of Using with Organizations	Delegated Administrator	Reference
IAM Identity Center	You can use IAM Identity Center to centrally manage your workforce identities and their access to multiple accounts in your organization. You can create identities for your entire enterprise at one go and give them single sign-on (SSO) access with managed permissions.	Supported	What Is IAM Identity Center?
Log Tank Service (LTS)	You can deploy a log aggregation center to aggregate logs across accounts. The organization administrator or delegated LTS administrator can copy the log streams of specified account in the organization on the LTS console to centrally store and analyze multi-account logs. This can meet the scenario-specific requirements for security compliance and centralized analysis.	Supported	Multi-Account Log Center

Service Name	Benefits of Using with Organizations	Delegated Administrator	Reference
SecMaster	You can apply workspace agencies to multiple accounts in a given organization. The organization administrator or delegated SecMaster administrator can create a workspace agency for one or more accounts in the organization.	Supported	Creating an Agency
IAM Access Analyzer	Access Analyzer provides organization-wide access analysis. The organization administrator or delegated administrator can create and manage access analyzers in a given organization, for example, to identify resources in the organization that are shared with external principals.	Supported	None

Service Name	Benefits of Using with Organizations	Delegated Administrator	Reference
Cloud Operations Center (COC)	Working with cross-account management of Organizations, COC allows an organization administrator or delegated service administrator to view the O&M situation and resource status of members in the organization and also to perform operations across accounts.	Supported	None

7.4 Specifying, Viewing, or Removing a Delegated Administrator

NOTICE

- Before removing the delegated administrator of the trusted service AOM, delete the multi-account instances on the AOM console and then access the Organizations console to start removal. Otherwise, the multi-account instances will continue retrieving the member accounts' metric data.
- Before removing the delegated administrator of the trusted service LTS, delete the configurations of multi-account log aggregation on the LTS console and then access the Organizations console to start removal. Otherwise, the multi-account log aggregation will continue retrieving the member accounts' logs.

Specifying a Delegated Administrator

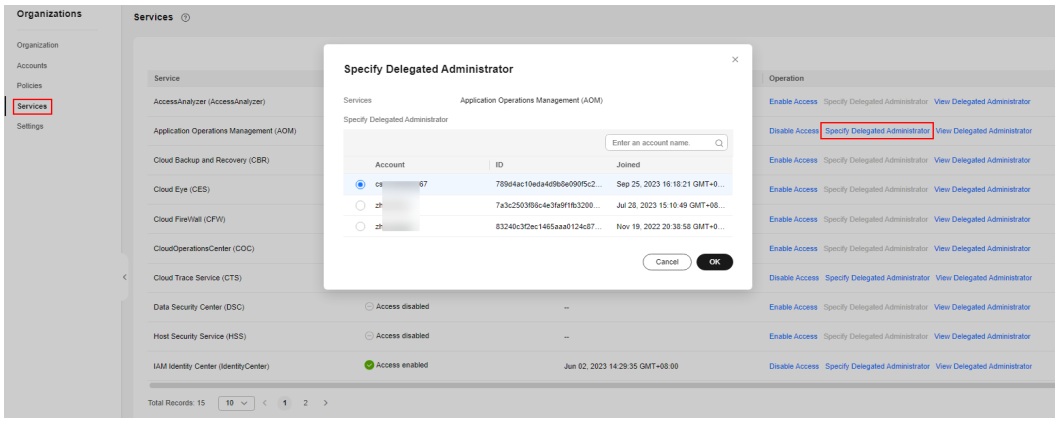
An account being closed cannot be specified as a delegated administrator.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Services** page, locate the target trusted service and click **Specify Delegated Administrator** in the **Operation** column.

Step 3 Select the account to be specified as the delegated administrator, and click **OK**.

Figure 7-4 Specifying a delegated administrator



----End

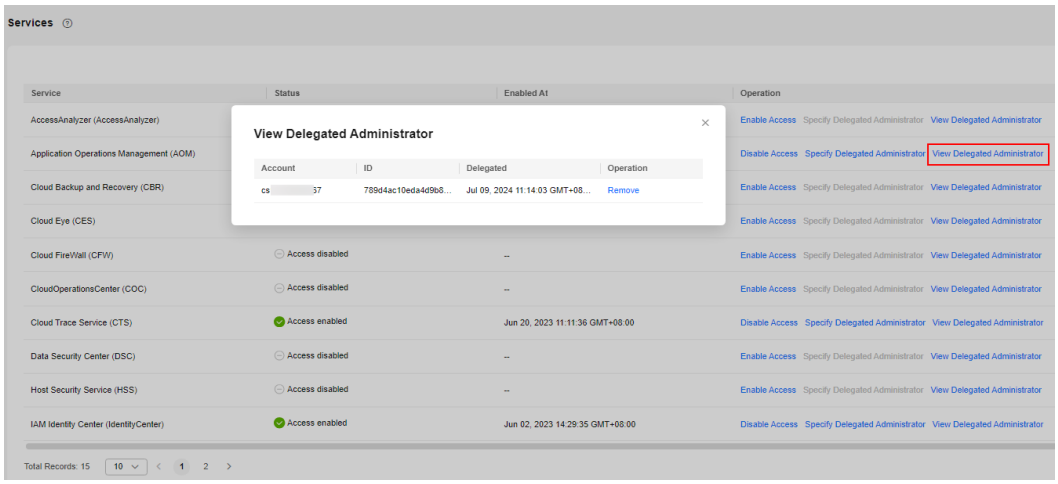
Viewing a Delegated Administrator

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Services** page, locate the target trusted service and click **View Delegated Administrator** in the **Operation** column.

Step 3 View the details about the delegated administrator of the trusted service.

Figure 7-5 Viewing details about a delegated administrator



----End

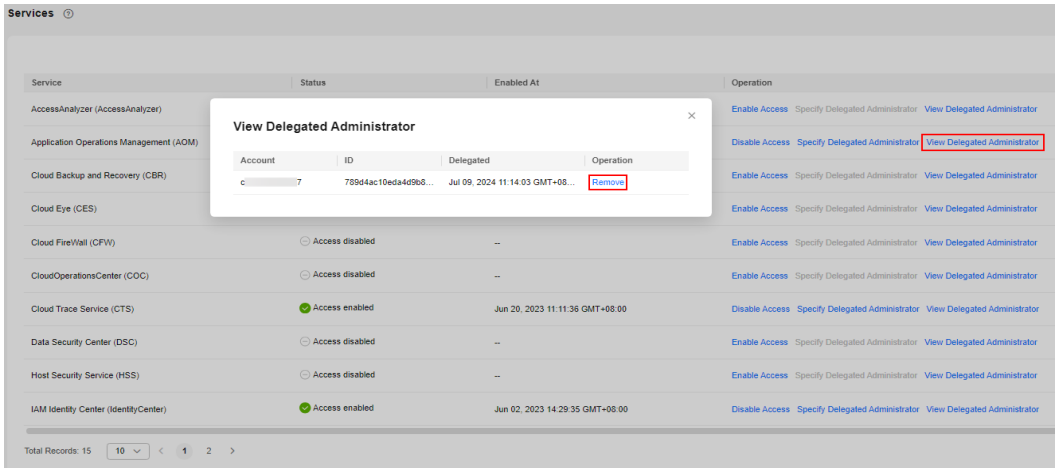
Removing a Delegated Administrator

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Services** page, locate the target trusted service and click **View Delegated Administrator** in the **Operation** column.

Step 3 In the displayed dialog box, click **Remove** in the **Operation** column.

Figure 7-6 Removing a delegated administrator



Step 4 Click **OK** in the displayed dialog box.

----End

8 Managing Tags

8.1 Overview of a Tag

Tag Introduction

A tag is a custom label you use to identify, categorize, and search for cloud resources. You can add tags to the following organization resources:

- Organization root
- Organizational units (OUs)
- Accounts
- Service control policies (SCPs)
- Tag policies

You can add tags at the following times:

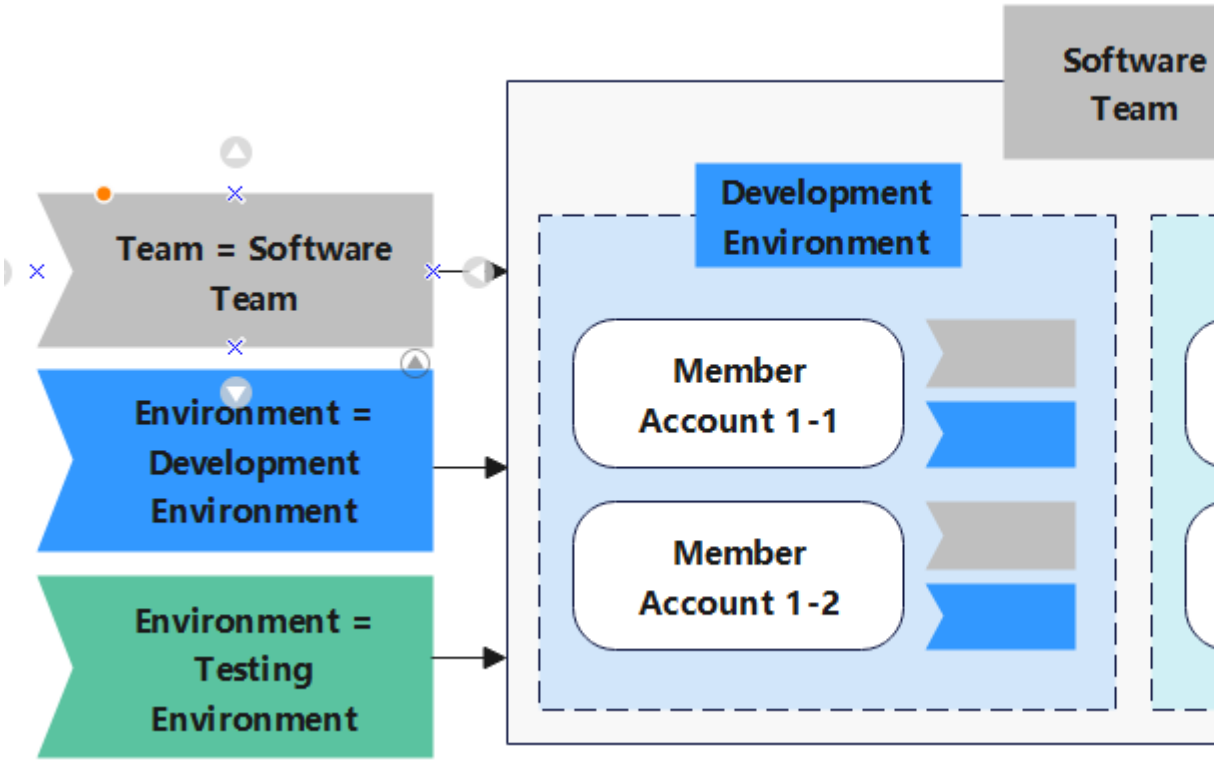
- When you create OUs, accounts, SCPs, or tag policies, you can add tags.
- When you view details about the organization root, OUs, accounts, SCPs, or tag policies, you can add, update, view, or delete tags on their details pages.

Basics of Tags

Tags help you to identify your cloud resources. When you have many cloud resources of the same type, you can use tags to classify them by dimension (for example, use, owner, or environment).

Figure 8-1 shows an example of how tags work. In this example, two tags were assigned to each member account. Each tag contains a key and a value defined by the user. The key of one tag is **Team**, and the key of another tag is **Environment**.

Figure 8-1 Example of tags



You can quickly search for and filter specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to track the owner and usage of each cloud resource, making resource management easier and faster.

Constraints on Using Tags

- The following basic naming and usage requirements apply to the key and value of a tag:

  Tag key:

  - Cannot be an empty string.
  - Contains 1 to 128 characters.
  - Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF).

  Tag value:

  - Can be an empty string.
  - Contains 1 to 225 characters.
  - Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF).
- Each cloud resource can have a maximum of 20 tags.
- For each resource, each tag key must be unique and can have only one tag value.

Helpful links:

- **Adding a Tag**: You can add tags for your OUs, accounts, SCPs, and tag policies.
- **Editing a Tag**: You can update the tag keys and values for OUs, accounts, SCPs, and tag policies.
- **Viewing Tag Details**: You can view the tags attached to OUs, accounts, SCPs, and tag policies.
- **Deleting a Tag**: You can delete tags from OUs, accounts, SCPs, and tag policies.

8.2 Adding a Tag

8.2.1 Adding a Tag for the Root, OUs, or Accounts

Scenario

The following describes how to add a tag for the root, OUs, or accounts.

Procedure

You add tags to the root, OUs, and accounts in the same way. The following uses adding tags to an OU as an example.

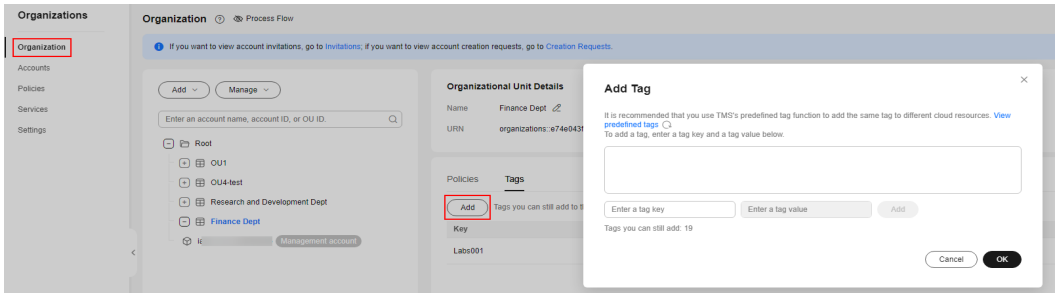
Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU you want to add a tag to, click the **Tags** tab in the pane on the right, and click **Add**.

Step 3 Enter a tag key and a tag value, click **Add**, and click **OK**.

You can select a predefined tag created in TMS from the drop-down lists. For details, see Creating Predefined Tags.

Figure 8-2 Adding a tag



----End

8.2.2 Adding a Tag for a Policy

Scenario

The following describes how to add a tag from custom SCPs and tag policies.

Procedure

The procedures for adding tags to SCPs and tag policies are similar. The following uses how to add tags to custom SCPs as an example.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Service control policies**.

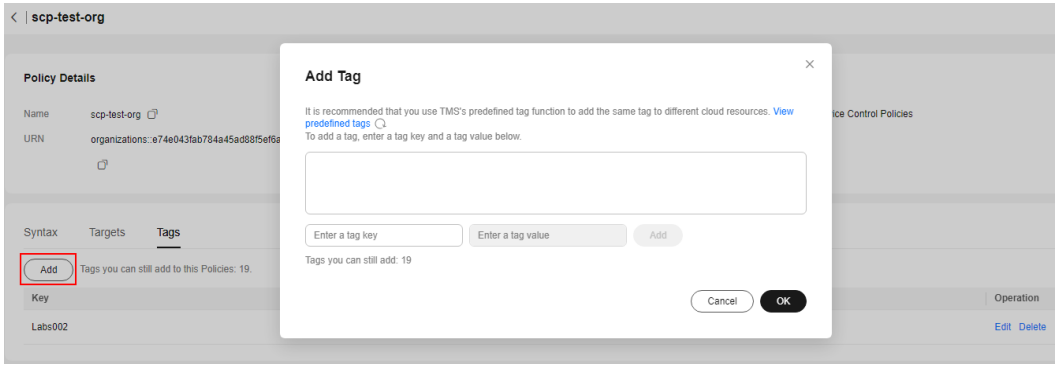
Step 3 Click the name of a policy to go to the policy details page.

Step 4 Click the **Tags** tab, and then click **Add**.

Step 5 Enter a tag key and a tag value, click **Add**, and click **OK**.

You can select a predefined tag created in TMS from the drop-down lists. For details, see Creating Predefined Tags.

Figure 8-3 Adding a tag



----End

8.3 Editing a Tag

8.3.1 Editing a Tag for the Root, OUs, or Accounts

Scenario

The following describes how to edit a tag for the root, OUs, or accounts.

Procedure

You edit tags for the root, OUs, and accounts in the same way. The following uses editing tags for an OU as an example.

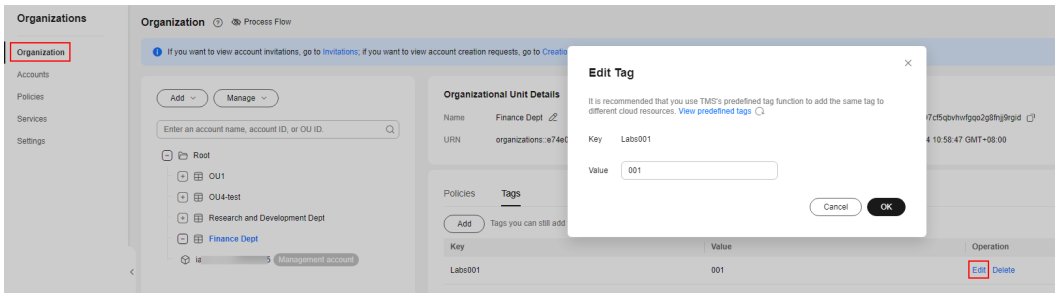
Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU you want to update a tag to, and click the **Tags** tab in the pane on the right. The list of tags is displayed.

Step 3 Locate the tag you want to edit and click **Edit** in the **Operation** column.

Step 4 Enter a new tag value, and click **OK** in the displayed dialog box.

Figure 8-4 Editing a tag



----End

8.3.2 Editing a Tag for a Policy

Scenario

The following describes how to edit a tag from custom SCPs and tag policies.

Procedure

The procedures for editing tags for SCPs and tag policies are similar. The following uses how to edit tags for custom SCPs as an example.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

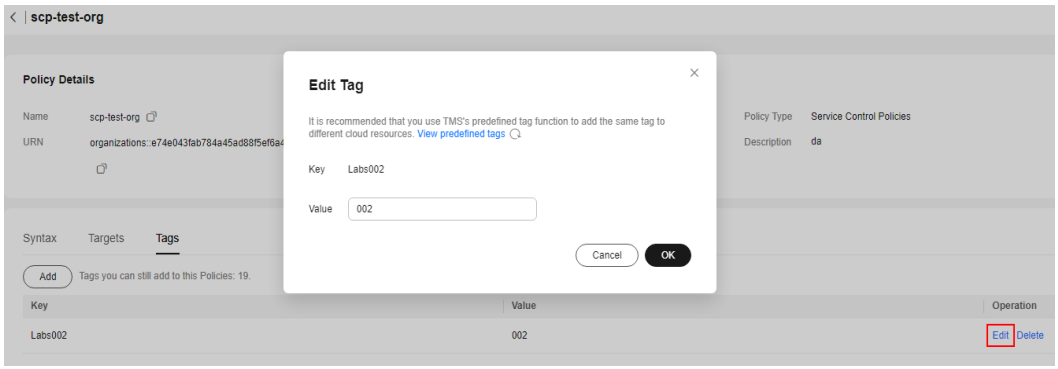
Step 2 On the **Policies** page, click **Service control policies**.

Step 3 Click the name of a policy to go to the policy details page.

Step 4 On the **Tags** page, locate the tag you want to edit and click **Edit** in the **Operation** column.

Step 5 Enter a new tag value, and click **OK** in the displayed dialog box.

Figure 8-5 Editing a tag



----End

8.4 Viewing Tag Details

8.4.1 Viewing Tag Details for the Root, OUs, or Accounts

Scenario

The following describes how to view tag details for the root, OUs, or accounts.

Procedure

You view tag details for the root, OUs, and accounts in the same way. The following uses viewing tag details of an OU as an example.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU whose tag details you want to view, and click the **Tags** tab in the pane on the right. The list of tags is displayed.

Step 3 View all tags attached to the OU in the tag list.

----End

8.4.2 Viewing Tag Details for a Policy

Scenario

The following describes how to view tag details for custom SCPs and tag policies.

Procedure

The procedures for viewing tag details for SCPs and tag policies are similar. The following uses how to view tag details for custom SCPs as an example.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

Step 2 On the **Policies** page, click **Service control policies**.

Step 3 Click the name of a policy to go to the policy details page.

Step 4 Click the **Tags** tab to view all the tags attached to the SCP.

----End

8.5 Deleting a Tag

8.5.1 Deleting a Tag from the Root, OUs, or Accounts

Scenario

The following describes how to delete a tag from the root, OUs, or accounts.

Procedure

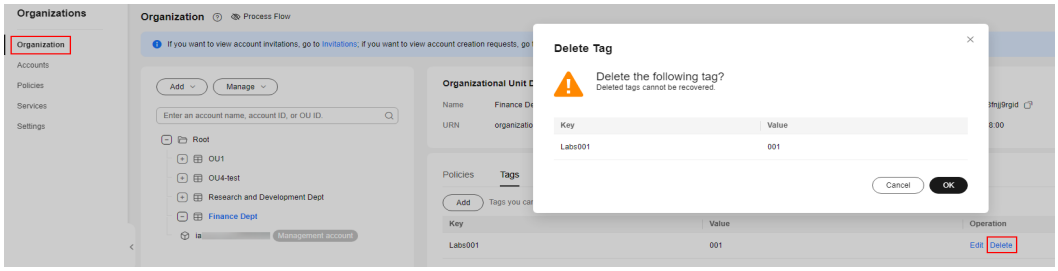
You delete tags from the root, OUs, and accounts in the same way. The following uses deleting a tag from an OU as an example.

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

Step 2 Select the OU whose tag you want to delete, and click the **Tags** tab in the pane on the right.

Step 3 Locate the tag you want to delete and click **Delete** in the **Operation** column. Then, click **OK** in the displayed dialog box.

Figure 8-6 Deleting a tag



----End

8.5.2 Deleting a Tag from a Policy

Scenario

The following describes how to delete a tag from custom SCPs and tag policies.

Procedure

The procedures for deleting tags from SCPs and tag policies are similar. The following uses how to delete tags from custom SCPs as an example.

Step 1 Log in to the management console as the organization administrator or using the management account, and navigate to the Organizations console.

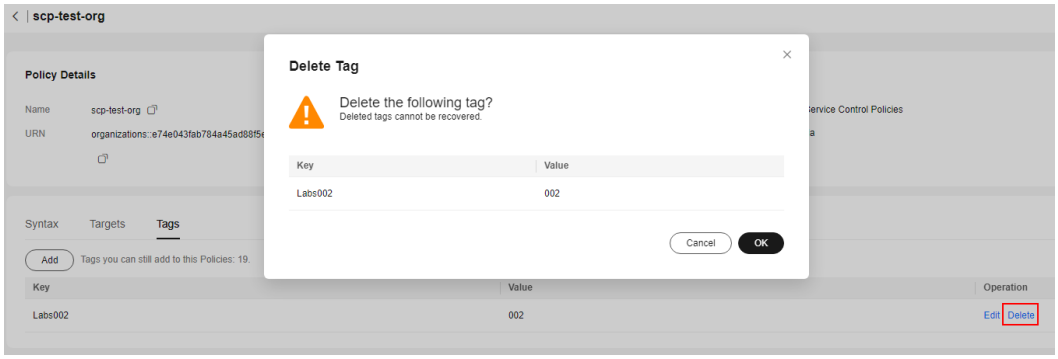
Step 2 On the **Policies** page, click **Service control policies**.

Step 3 Click the name of a policy to go to the policy details page.

Step 4 On the **Tags** page, locate the tag you want to delete and click **Delete** in the **Operation** column.

Step 5 Click **OK** in the displayed dialog box.

Figure 8-7 Deleting a tag



----End

9 CTS Auditing

9.1 Supported Organizations Operations

With Cloud Trace Service (CTS), you can record Organizations operations for later query, auditing, and backtracking.

Table 9-1 Organizations operations that can be recorded by CTS

Operation	Resource Type	Event Name
Creating an organization	Organization	createOrganization
Deleting an organization	Organization	celeteOrganization
Leaving an organization	Organization	leaveOrganization
Creating an OU	OrganizationUnit	createOrganizationalUnit
Updating an OU	OrganizationUnit	updateOrganizationalU-nit
Deleting an OU	OrganizationUnit	deleteOrganizationalUnit
Inviting an account	Account	inviteAccount
Creating an account	Account	createAccount
Closing an account	Account	closeAccount
Updating an account	Account	updateAccount
Moving an account	Account	moveAccount
Removing an account	Account	removeAccount
Accepting an invitation	Handshake	acceptHandshake
Declining an invitation	Handshake	declineHandshake
Canceling an invitation	Handshake	cancelHandshake

Operation	Resource Type	Event Name
Enabling a trusted service	TrustedService	enableTrustedService
Disabling a trusted service	TrustedService	disableTrustedService
Configuring a delegated administrator	DelegatedAdministrator	registerDelegatedAdministrator
Removing a delegated administrator	DelegatedAdministrator	deregisterDelegatedAdministrator
Creating a policy	Policy	createPolicy
Updating a policy	Policy	updatePolicy
Deleting a policy	Policy	deletePolicy
Enabling a policy type	Policy	enablePolicyType
Disabling a policy type	Policy	disablePolicyType
Attaching a policy	Policy	attachPolicy
Detaching a policy	Policy	detachPolicy
Adding a tag	• Account • OrganizationUnit • Policy • Root • Tag	tagResource
Deleting a tag	• Account • OrganizationUnit • Policy • Root • Tag	untagResource

9.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in Object Storage Service (OBS) buckets. Cloud Trace Service (CTS) stores operation records (traces) generated in the last seven days.

This section describes how to query or export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, you must configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console one minute later and query data traces five minutes later.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - **Enterprise Project ID**: Enter an enterprise project ID.
   - **Access Key**: Enter a temporary or permanent access key ID.

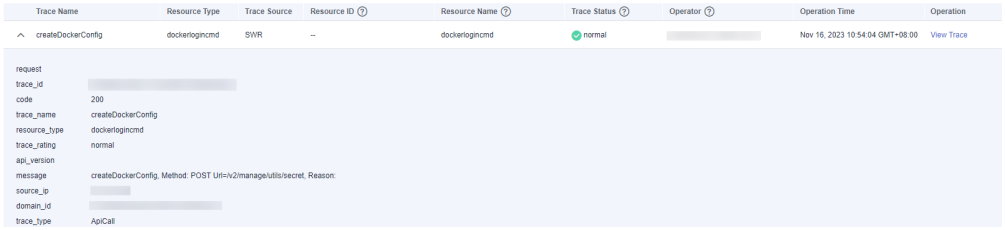
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.

5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
   - Enter any keyword in the search box and press **Enter** to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
   - Click to view the latest information about traces.
   - Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see Trace Structure and Example Traces.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

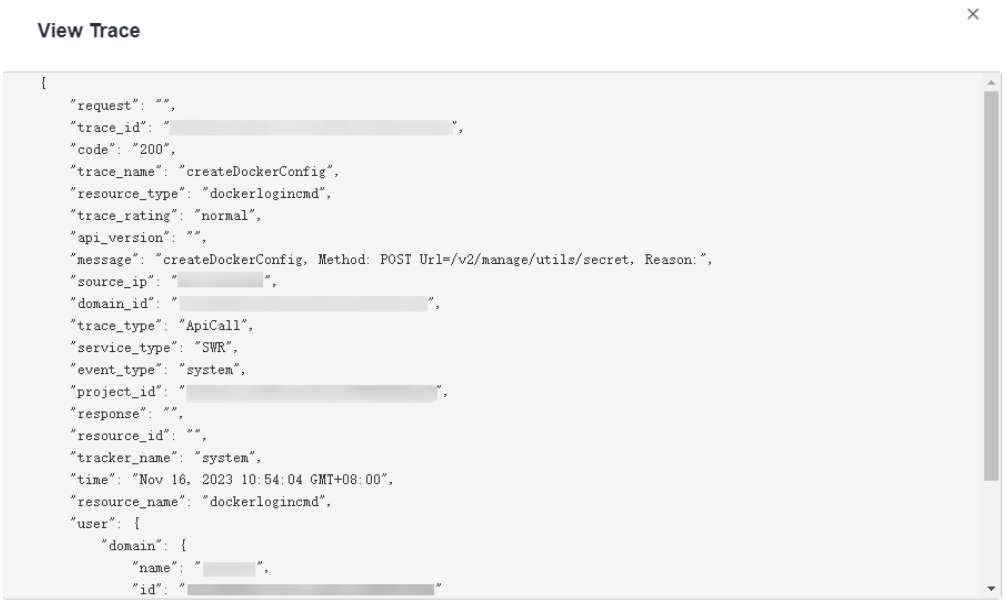
Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click to view the latest information about traces.

8. Click ⌄ on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see Trace Structure and Example Traces in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

10 Adjusting Quotas

What Is Quota?

A quota is a limit on the quantity or capacity of a certain type of service resources that a user can use, for example, the maximum number of OUs you can create or the number of member accounts you can invite to an organization.

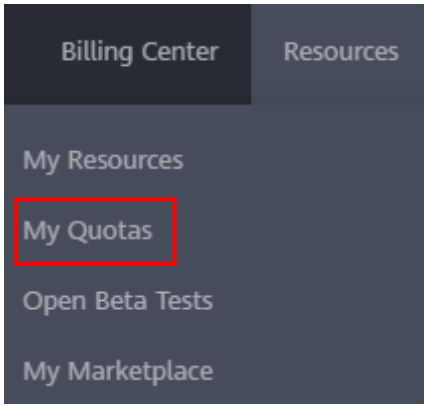
If a quota cannot meet your needs, apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click in the upper left corner and select a region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** page is displayed.

   Figure 10-1 My Quotas

4. On the **Service Quota** page, view the used and total quotas of each type of resources.

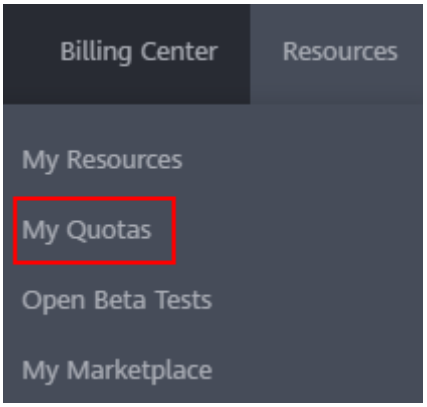
   If the quota cannot meet your service requirements, increase the quota.

How Do I Increase My Quota?

1. Log in to the management console.

2. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 10-2 My Quotas

3. Click **Increase Quota**.
4. On the **Create Service Ticket** page, set the parameters.
   In the **Problem Description** area, enter the required quota and the reason for the quota adjustment.
5. Read the agreements and confirm that you agree to them, and then click **Submit**.

