

# Identity and Access Management (IAM 2.0)

## 8.5.1

# Service Overview

<b>Issue</b>	01
<b>Date</b>	2026-05-14



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

---

# Contents

---

<b>1 What Is IAM?</b> .....	<b>1</b>
<b>2 Basic Concepts</b> .....	<b>4</b>
<b>3 Functions</b> .....	<b>9</b>
<b>4 Supported Cloud Services</b> .....	<b>15</b>
<b>5 Permissions</b> .....	<b>27</b>
<b>6 Security</b> .....	<b>35</b>
6.1 Shared Responsibilities.....	35
6.2 Authentication and Access Control.....	37
6.2.1 Identity Authentication.....	37
6.2.2 Configuring Access Control.....	39
6.3 Data Protection.....	40
6.3.1 IAM Side.....	40
6.3.2 Tenant Side.....	42
6.4 Resilience.....	42
6.5 Audit and Monitoring.....	42
6.6 Certificates.....	43
<b>7 Notes and Constraints</b> .....	<b>45</b>

# 1 What Is IAM?

---

Huawei Cloud Identity and Access Management (IAM 2.0) provides permissions management to help you securely control access to your cloud services and resources.

IAM is free of charge. You pay only for the cloud resources in your account.

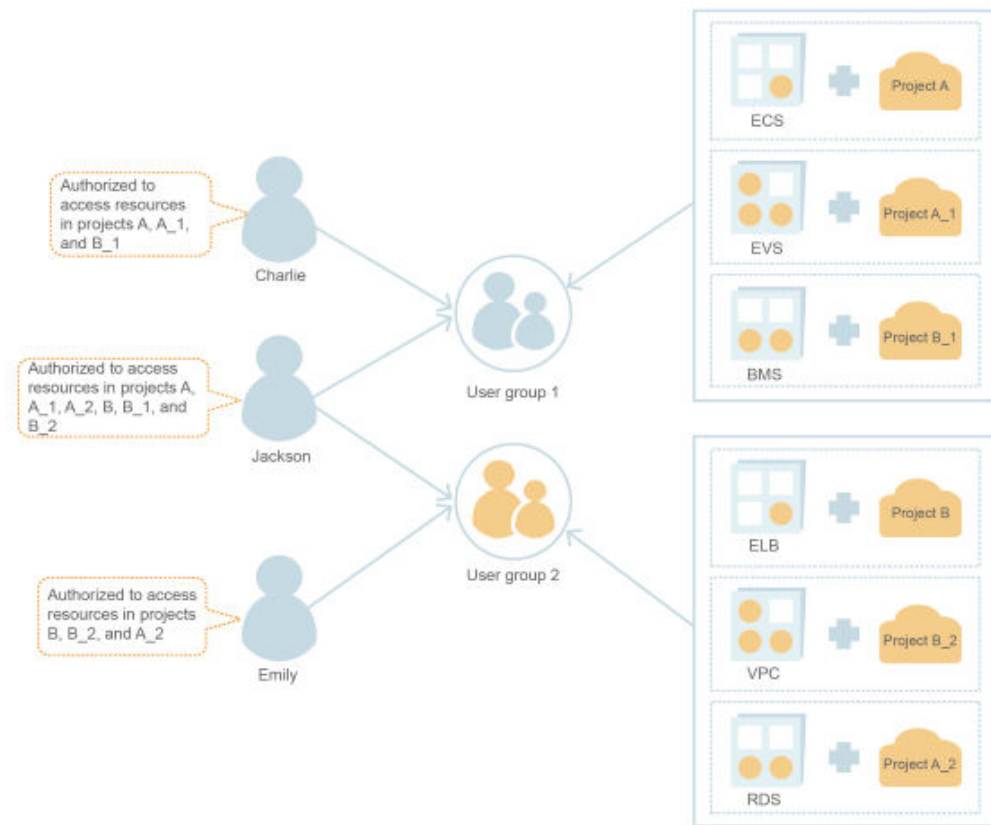
## Advantages

### Fine-grained access control for Huawei Cloud resources

When you successfully sign up for Huawei Cloud, the system automatically creates an account for you. Your account owns resources and pays for the use of these resources. Your account has full access permissions for your cloud services and resources.

You may purchase multiple Huawei Cloud resources, such as Elastic Cloud Servers (ECSs), Elastic Volume Service (EVS) disks, and Bare Metal Servers (BMSs), for different teams or applications in your enterprise. You can use your account to create IAM users for the team members or applications and grant them permissions required to complete specific tasks. The IAM users use their own usernames and passwords to log in to Huawei Cloud. IAM users enable fine-grained permission control when multiple users collaborate on the same account.

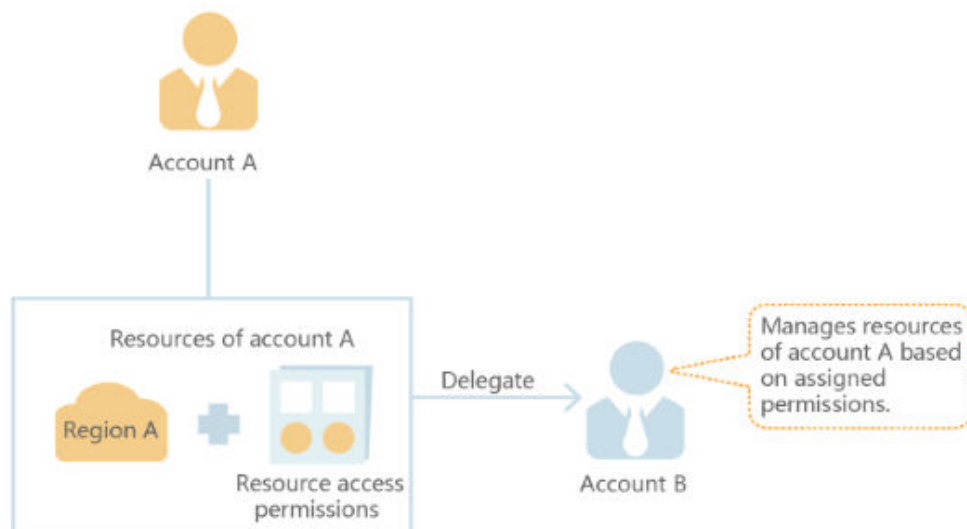
In addition to IAM, you can use Enterprise Management to control access to cloud resources. Enterprise Management supports more fine-grained permissions management and enterprise project management. You can choose either IAM or Enterprise Management to suit your requirements. For details, see [What Are the Differences Between IAM and Enterprise Management?](#)



### Cross-account resource access delegation

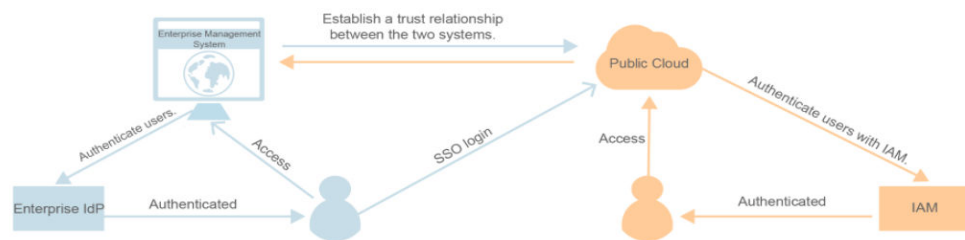
If you purchase multiple Huawei Cloud resources, you can delegate another account to manage some of your resources for efficient O&M.

For example, you can create an agency for a professional O&M company to allow them to manage specific resources with its own account. If the delegation changes, you can modify or revoke the delegated permissions at any time. In the following figure, account A is the delegating party, and account B is the delegated party.



### Federated access to Huawei Cloud with existing enterprise accounts (identity federation)

If your enterprise has an identity system, you can create an identity provider (IdP) in IAM to provide single sign-on (SSO) access to Huawei Cloud for employees in your enterprise. The IdP establishes a trust relationship between your enterprise and Huawei Cloud, allowing the employees to access Huawei Cloud using their existing accounts.



### Access Methods

You can access IAM using either of the following methods:

- **Management console**  
Access IAM through the management console — a browser-based visual interface. For details, see [Accessing the IAM Console](#).
- **REST APIs**  
Access IAM using REST APIs. For details, see [API Reference](#).

If you want to view, audit, and track the records of key operations performed on IAM, enable Cloud Trace Service (CTS). For details, see [Key IAM Operations Supported by CTS](#).

# 2 Basic Concepts

---

The following are basic concepts that you need to understand before you get started with the IAM service.

## Account

An account is created after you successfully sign up for Huawei Cloud. Your account owns your Huawei Cloud resources and pays for the use of these resources. It has full access permissions for your cloud services and resources. You can use your account to perform operations such as resetting the login password and assigning permissions to IAM users. We charge your account for the resources used by the IAM users in the account.

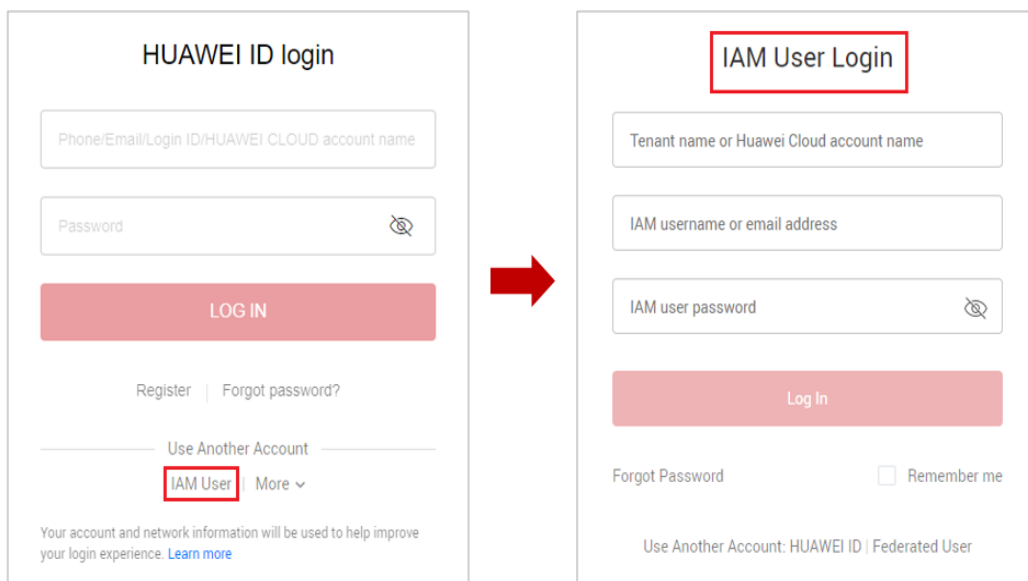
You cannot modify or delete your account in IAM, but you can do so in My Account.

## IAM User

You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (password and access keys) and uses cloud resources based on the assigned permissions. IAM users cannot make payments themselves (they do not have bills). You can use your account to pay for the resources they use.

If a user forgot their password, the user can reset the password by referring to [What Should I Do If I Forgot My Password?](#)

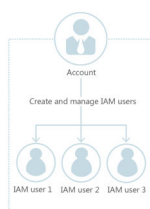
Figure 2-1 IAM user login



## Relationship Between an Account and Its IAM Users

An account and its IAM users have a parent-child relationship. The account owns the resources and pays for the resources used by IAM users. It has full permissions for these resources. IAM users are created by an account, and they only have the permissions granted by the account. The account can modify or revoke the IAM users' permissions at any time. IAM users cannot make payments themselves. The account pays for the resources they use.

Figure 2-2 Account and IAM users



## Administrator

IAM is intended for administrators, including:

- Account administrator (with full permissions for all services, including IAM)
- IAM users added to the **admin** group (with full permissions for all services, including IAM)
- IAM users assigned the **Security Administrator** permissions (with permissions to access IAM)

## Authorization

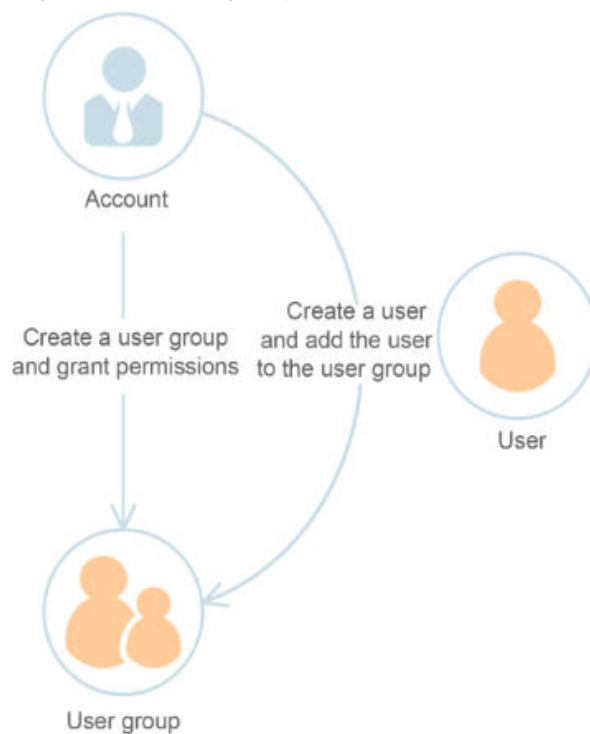
Authorization is the process of using policies to grant IAM users permissions required to perform specific tasks, such as managing ECS resources in your account.

## User Group

An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users. This makes it easier to manage the permissions for those users. IAM users added to a user group automatically inherit the permissions from the group. If a user is added to multiple user groups, the user inherits the permissions from all these groups.

There is a default user group **admin**. It has all the permissions required to use all of the cloud resources. IAM users in this group can perform operations on all resources, including but not limited to creating user groups and users, assigning permissions, and managing resources.

**Figure 2-3** User group and users



## Permissions

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only the permissions

required to manage ECSs of a certain type. IAM supports both system-defined and custom policies.

- A system-defined policy defines the common actions of a cloud service. You can use system-defined policies to assign permissions to user groups. You cannot modify such policies. If you need to assign permissions for a specific service to a user group or agency on the IAM console but cannot find corresponding policies, the service does not support permissions management through IAM. You can [submit a service ticket](#) to request that permissions for the service be made available in IAM.
- Custom policies function as a supplement to system-defined policies. You can create custom policies using the actions supported by cloud services for more refined access control. You can create custom policies in the visual editor or in JSON view.

**Figure 2-4** Example permissions

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "apm:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## Credentials

Huawei Cloud uses credentials to verify the identities of users when they attempt to access through the console or APIs. Credentials can be passwords or access keys. You can manage your own credentials and your IAM users' credentials.

- Password: A common credential for logging in to the management console or calling APIs.
- Access key: An access key ID/secret access key (AK/SK) pair. You can use it to call APIs, but it does not support console login. Each access key provides a signature for cryptographic authentication to ensure that access requests are secret, complete, and correct.

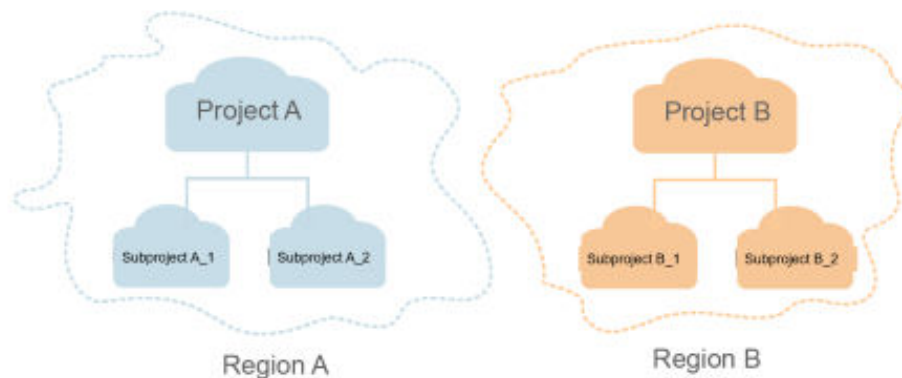
## Virtual MFA Device

A virtual MFA device is an application that generates 6-digit verification codes in compliance with the Time-based One-time Password Algorithm (TOTP) standard. MFA devices can be hardware- or software-based. Huawei Cloud only supports software-based virtual MFA devices, which are application programs running on smart devices such as mobile phones. For details about how to use virtual MFA devices, see [Virtual MFA Device](#).

## Project

A region corresponds to a project. Default projects are defined to group and physically isolate compute, storage, and network resources across regions. You can grant users permissions in a default project to access all resources in the region associated with the project. If you need more refined access control, you can create subprojects under a default project and purchase resources in subprojects. Then you can assign required permissions for users to access only resources in specific subprojects.

**Figure 2-5** Projects



## Enterprise Project

Enterprise projects allow you to group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. An enterprise project can contain resources of multiple regions, and you can easily add resources to or remove resources from enterprise projects.

For details about how to obtain enterprise project IDs and features, see the [Enterprise Management User Guide](#).

## Agency

You can use an agency to establish a trust relationship between your account and another account or a cloud service.

- Account delegation: You can delegate another account to implement O&M on your resources based on assigned permissions.
- Cloud service delegation: Huawei Cloud services interwork with each other, and some cloud services are dependent on other services. You can create an agency to delegate a cloud service to access other services and implement O&M.

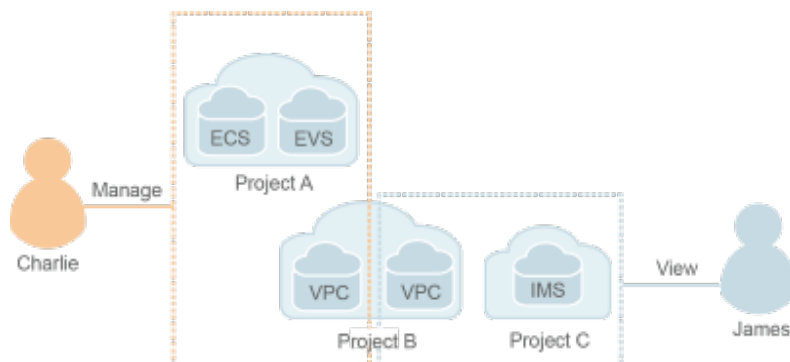
# 3 Functions

IAM provides a variety of functions for you to secure access to your resources.

## Refined Permissions Management

You can grant IAM users permissions to manage different resources in your account. As shown in the following figure, you can grant Charlie permission to manage Virtual Private Cloud (VPC) resources in project B, and only grant James permission to view VPC resources in project B.

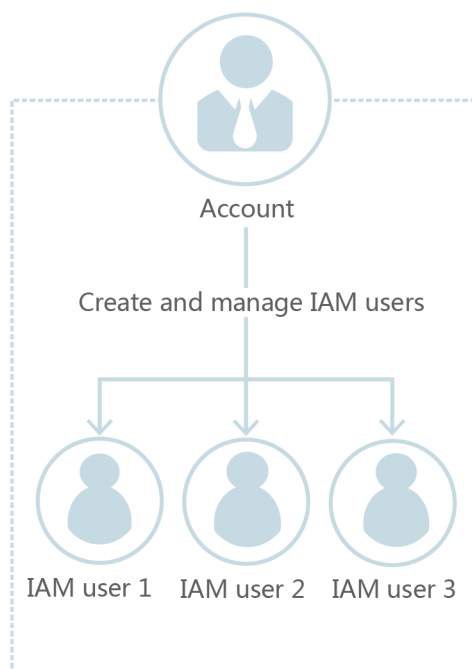
**Figure 3-1** Permissions management model



## IAM User Management

You can use your account to create IAM users and assign permissions for specific resources. Each IAM user has their own identity credentials (password and access keys) and uses cloud resources based on the assigned permissions. IAM users do not own resources.

**Figure 3-2** Relationship between an account and its IAM users

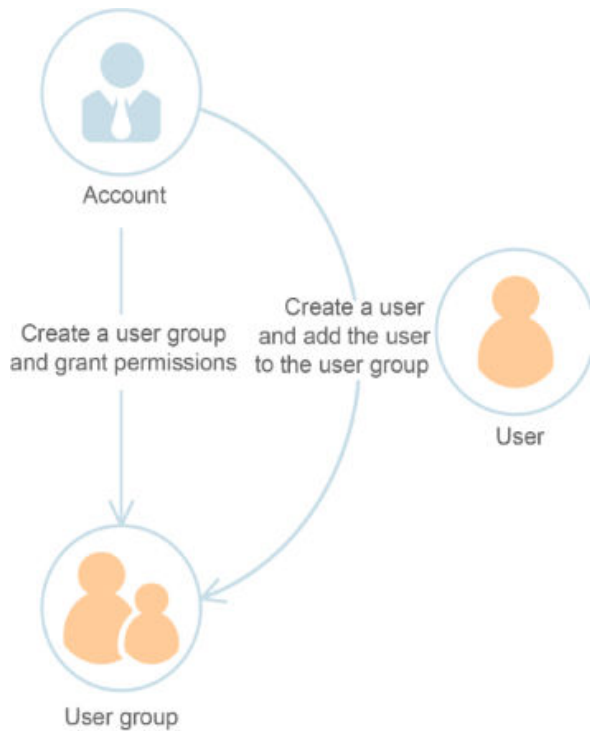


## User Group Management

An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users. This makes it easier to manage the permissions for those users. IAM users added to a user group automatically inherit the permissions from the group. If a user is added to multiple user groups, the user inherits the permissions from all these groups. To change the permissions of a user, you can remove the user from the original groups or add the user to other groups.

There is a default user group **admin**. It has all the permissions required to use all of the cloud resources. IAM users in this group can perform operations on all resources, including but not limited to creating user groups and users, assigning permissions, and managing resources.

**Figure 3-3** User group and users



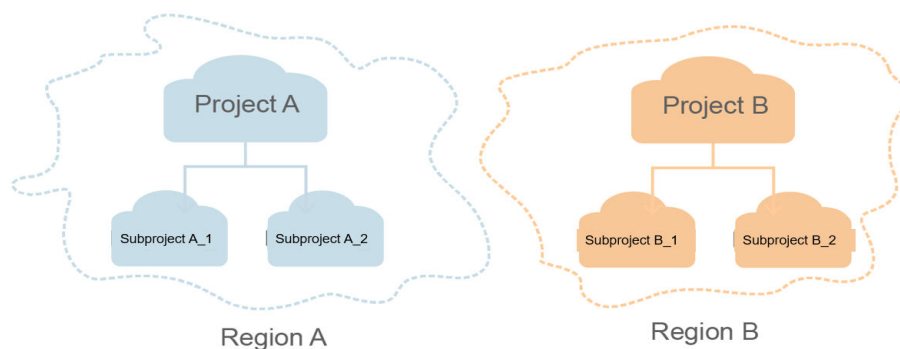
## Custom Policies

You can create custom policies to supplement system-defined policies and implement more refined access control. Specifically, you can allow or deny a user's operations on a resource type under certain conditions.

## Project Management

A region corresponds to a project. Default projects are defined to group and physically isolate compute, storage, and network resources across regions. You can grant users permissions in a default project to access all resources in the region associated with the project. If you need more refined access control, you can create subprojects under a default project and purchase resources in subprojects. Then you can assign required permissions for users to access only resources in specific subprojects.

**Figure 3-4** Project isolation model

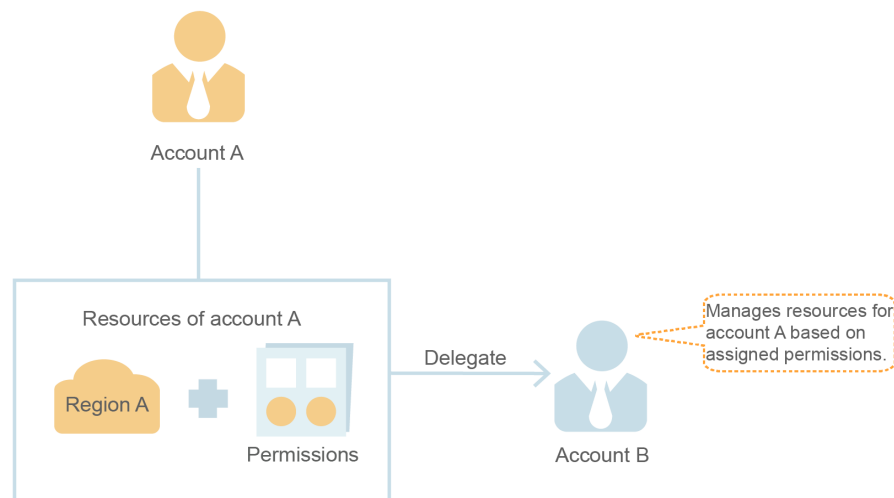


## Agency Management

IAM enables you to delegate resource access to another account or a specific cloud service.

- **Account agency:** You can delegate another Huawei Cloud account to implement O&M on your resources based on assigned permissions. The following is an example to show how to delegate resource access to another account. In this example, account A is the delegating party and account B is the delegated party.

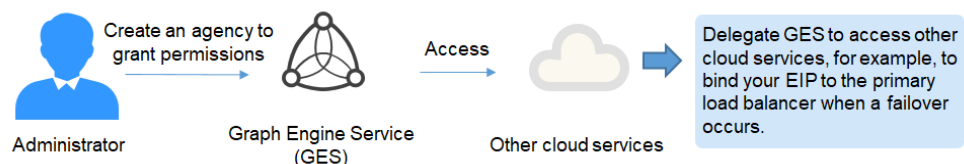
**Figure 3-5** (Account A) Creating an agency



- **Cloud service agency:** Huawei Cloud services interwork with each other, and some cloud services are dependent on other services. You can create an agency to delegate a cloud service to access other services and implement O&M.

The following takes a Graph Engine Service (GES) agency as an example. The agency allows GES to use other cloud services, for example, to bind your EIP to the primary load balancer if a failover occurs.

**Figure 3-6** Cloud service agency



## Account Security Settings

Login authentication and password policies and access control list (ACL) improve security of user information and system data.

## Multi-Factor Authentication

Multi-factor authentication (MFA) is a popular method that adds an additional layer of authentication on top of the username and password. If MFA is enabled,

you need to enter the username and password (first factor) as well as a verification code (second factor) when performing certain operations. These factors together keep your account and resources secure.

MFA mainly serves two purposes: login authentication and operation protection. With login authentication enabled, a username, password, and verification code are all required on the login page. With operation protection enabled, a verification code is required to confirm any critical operation.

## Federated Identity Authentication

Huawei Cloud provides identity federation based on Security Assertion Markup Language (SAML) or OpenID Connect. This function allows users in your enterprise management system to access Huawei Cloud through single sign-on (SSO).

## Audit

Cloud Trace Service (CTS) records operations performed on cloud resources in your account. The operation logs can be used to perform security analysis, track resource changes, perform compliance audits, and locate faults.

It is recommended that the administrator enables CTS to record key IAM operations, such as creating and deleting users.

## Best Practices for Using IAM

To establish secure access to your Huawei Cloud resources, follow the best practices for the IAM service. For details, see [Best Practices for Using IAM](#).

## APIs

IAM provides Representational State Transfer (REST) APIs, which you can call using HTTPS requests. For details, see [Making an API Request](#).

## SDKs

IAM provides a user management mechanism that is suitable for enterprises, and enables you to assign permissions for different resources and operations to enterprise members. With the SDKs, you can easily call IAM APIs to create upper-layer applications on Huawei Cloud. Currently, Java, Python, .NET, and Go SDKs are available.

## Secure Access

Instead of sharing your password with others, you can create IAM users for employees or applications in your organization. Then, you generate identity credentials for them to securely access specific resources based on assigned permissions.

## Eventual Consistency

IAM may not apply your operations immediately, such as creating users and user groups and assigning permissions. It takes time to replicate data across different

servers in Huawei Cloud's data centers around the world. Do not perform any other operations until IAM has applied the operations you just made.

# 4 Supported Cloud Services

---

IAM provides identity authentication and permissions management for other Huawei Cloud services. Users created in IAM can access these services based on assigned permissions. For all permissions of the services supported by IAM, see [System-defined Permissions](#). For services that are not supported by IAM, you can only use your account to access these services.

The following tables in this topic list the IAM-supported services. You can refer to the table heading descriptions below before viewing the table content.

- **Service:** Name of a cloud service that supports permissions management using IAM.
- **Scope:** The region where access permissions for a service can be assigned using IAM.
  - **Global regions:** Services deployed without specifying physical regions are global services. You must assign permissions for these services in global regions. Users do not need to switch regions when they access these services.
  - **Specific regions:** Services deployed for specific regions are project-level services. Permissions for these services need to be assigned in specific regions and take effect only for these regions. Users need to switch to one of these regions when they access the services.
- **Console:** Whether a service supports permissions management using the IAM console.
- **API:** Whether a service supports permissions management using APIs.
- **Cloud Service Agency:** Whether you can delegate a service to access and manage other cloud services on your behalf.
- **Policy:** Whether a service supports policy-based permissions management. A policy is a set of permissions in JSON format that allow or deny specific operations on specific cloud resources.
- **Enterprise Project:** Whether a service supports authorization by enterprise project. For details about enterprise projects, see [Enterprise Management User Guide](#).

## NOTE

√: supported; x: not supported

## Compute

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Elastic Cloud Server (ECS)	Specific regions	√	√	√	√	√
Bare Metal Server (BMS)	Specific regions	√	√	√	√	√
Auto Scaling (AS)	Specific regions	√	√	x	√	√
Cloud Phone Host (CPH)	Specific regions	√	√	x	x	x
Image Management Service (IMS)	Specific regions	√	√	√	√	√
FunctionGraph	Specific regions	√	√	√	x	√
Dedicated Host (DeH)	Specific regions	√	x	x	√	√

## Storage

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Elastic Volume Service (EVS)	Specific regions	√	√	x	√	√
Business Recovery Service (BRS)	Specific regions	√	√	x	x	x
Cloud Server Backup Service (CSBS)	Specific regions	√	√	x	x	x
Volume Backup Service (VBS)	Specific regions	√	√	x	x	x
Object Storage Service (OBS)	Global regions	√	√	√	√	√

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Scalable File Service (SFS)	Specific regions	√	√	x	√	√
Content Delivery Network (CDN)	Global regions	√	√	x	√	√
Cloud Backup and Recovery (CBR)	Specific regions	√	√	x	√	√

## Network

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Virtual Private Cloud (VPC)	Specific regions	√	√	x	√	√
Elastic IP Address (EIP)	Specific regions	√	√	x	√	√
Elastic Load Balance (ELB)	Specific regions	√	√	x	√	√
Domain Name Service (DNS)	<ul style="list-style-type: none"> <li>Global regions: public zone, PTR record, and custom line</li> <li>Specific regions: private zone and resolver</li> </ul>	√	√	x	x	√
NAT Gateway	Specific regions	√	√	x	√	√
Direct Connect	Specific regions	√	x	x	x	x
Virtual Private Network (VPN)	Specific regions	√	x	x	√	x

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Cloud Connect (CC)	Specific regions	√	x	x	√	√
VPC Endpoint (VPCEP)	Specific regions	√	√	x	x	x

## Containers

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Cloud Container Engine (CCE)	Specific regions	√	√	x	√	√
Cloud Container Instance (CCI)	Specific regions	√	√	x	√	√
Software Repository for Container (SWR)	Specific regions	√	√	x	√	x
Gene Container Service (GCS)	Specific regions	√	√	x	√	√

## Database

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Relational Database Service (RDS)	Specific regions	√	√	x	√	√
Document Database Service (DDS)	Specific regions	√	x	x	√	√

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Distributed Database Middleware (DDM)	Specific regions	√	√	x	√	√
Data Replication Service (DRS)	Specific regions	√	√	x	√	√
Data Admin Service (DAS)	Specific regions	√	x	x	x	x
GeminiDB	Specific regions	√	√	x	√	√

## Security & Compliance

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Anti-DDoS	Specific regions	√	√	x	x	x
Advanced Anti-DDoS (AAD)	Specific regions	√	√	√	x	√
Cloud Native Anti-DDoS (CNAD)	Global regions	√	√	x	√	x
Web Application Firewall (WAF)	Specific regions	√	x	x	x	√
Cloud Firewall (CFW)	Specific regions	√	x	x	√	x
Vulnerability Scan Service (VSS)	Specific regions	√	x	x	x	x
Host Security Service (HSS)	Specific regions	√	x	x	x	√
Database Security Service (DBSS)	Specific regions	√	x	x	√	x

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Data Encryption Workshop (DEW)	Specific regions	√	√	x	x	x
SSL Certificate Manager (SCM)	Global regions	√	√	x	√	x
Container Guard Service (CGS)	Specific regions	√	x	x	√	x
Cloud Bastion Host (CBH)	Specific regions	√	√	x	√	x
Data Security Center (DSC)	Specific regions	√	√	x	√	x

## Management & Governance

Service	Scope	Console	API	Cloud Service Agency	Fine-Grained Policy	Enterprise Project
Identity and Access Management (IAM)	Global regions	√	√	x	√	x
Cloud Eye	Specific regions	√	√	x	√	√
Cloud Trace Service (CTS)	Specific regions	√	√	x	x	x
Application Performance Management (APM)	Specific regions	√	√	x	√	√
Application Operations Management (AOM)	Specific regions	√	√	x	√	√
Log Tank Service (LTS)	Specific regions	√	√	x	√	√

Service	Scope	Console	API	Cloud Service Agency	Fine-Grained Policy	Enterprise Project
Tag Management Service (TMS)	Global regions	√	√	x	x	x
Cloud Operations Center (COC)	Global regions	√	√	√	√	√

## Application

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
ServiceStage	Specific regions	√	√	x	x	x
Distributed Cache Service (DCS)	Specific regions	√	√	√	√	√
Distributed Message Service for Kafka (DMS for Kafka)	Specific regions	√	√	x	√	√
Distributed Message Service for RabbitMQ (DMS for RabbitMQ)	Specific regions	√	√	x	√	√
Distributed Message Service for RocketMQ (DMS for RocketMQ)	Specific regions	√	√	x	√	√
Simple Message Notification (SMN)	Specific regions	√	√	x	x	√
Cloud Service Engine (CSE)	Specific regions	√	√	x	x	√
CodeArts PerfTest	Specific regions	√	√	x	x	x

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
API Gateway	Specific regions	√	√	x	x	√
Blockchain Service (BCS)	Specific regions	√	√	x	√	√

## DeC

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Dedicated Distributed Storage Service (DSS)	Specific regions	√	√	x	√	x

## Migration

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Server Migration Service (SMS)	Global regions	√	x	x	√	x
Object Storage Migration Service (OMS)	Specific regions	√	x	x	x	x
Cloud Data Migration (CDM)	Specific regions	√	√	√	√	√

## Intelligent Edge

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
CloudLake	Global regions	√	x	x	√	x

## EI

Service	Scope	Console	API	Cloud Service Agency	Fine-Grained Policy	Enterprise Project
ModelArts	Specific regions	√	√	√	√	√
DataArts Studio	Specific regions	√	√	√	√	x
MapReduce Service (MRS)	Specific regions	√	√	x	√	√
Data Warehouse Service (DWS)	Specific regions	√	√	√	√	√
CloudTable	Specific regions	√	√	x	x	√
Data Lake Insight (DLI)	Specific regions	√	√	x	x	√
Data Ingestion Service (DIS)	Specific regions	√	√	√	x	√
Cloud Search Service (CSS)	Specific regions	√	√	√	x	√
Graph Engine Service (GES)	Specific regions	√	√	√	x	√
Content Moderation	Specific regions	√	√	x	√	x
Conversational Bot Service (CBS)	Specific regions	√	√	x	x	x
Huawei HiLens	Specific regions	√	x	x	√	x

Service	Scope	Console	API	Cloud Service Agency	Fine-Grained Policy	Enterprise Project
Trusted Intelligent Computing Service (TICS)	Specific regions	√	x	x	√	x

## Enterprise Applications

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Workspace	Specific regions	√	√	x	x	x
ROMA Connect	Specific regions	√	√	√	√	√
CloudSite	Specific regions	√	x	√	√	x

## Cloud Communications

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Voice Call	Specific regions	√	√	√	x	x
Message & SMS	Specific regions	√	√	√	√	x
Private Number	Specific regions	√	√	√	√	x

## Video

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Media Processing Center (MPC)	Specific regions	√	√	√	x	x
Video on Demand (VOD)	Specific regions	√	√	√	√	x

## Development and O&M

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
CodeArts	Specific regions	√	x	x	√	√
CodeArts Req	Specific regions	√	√	x	√	x
CloudIDE	Specific regions	√	√	x	√	x

## User Support

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
My Account	Specific regions	√	x	x	√	x
Billing Center	Specific regions	√	x	x	√	x
Resource Center	Specific regions	√	x	x	√	x

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
<b>Enterprise Project Management Service (EPS)</b>	Global regions	√	√	x	√	x
<b>Service Tickets</b>	Global regions	√	√	x	x	x
ICP License Service	Global regions	√	x	x	x	x
Professional Services	Global regions	√	x	x	√	x

## Other

Service	Scope	Console	API	Cloud Service Agency	Policy	Enterprise Project
Message Center	Specific regions	√	x	x	√	x

# 5 Permissions

---

You can use IAM to grant specific permissions to access your IAM resources to different employees in your enterprise. IAM provides identity authentication, fine-grained permissions management, and access control. It helps you secure access to your Huawei Cloud resources.

With IAM, you can create IAM users and grant them permissions to access only specific resources. For example, you can grant permissions to allow certain project planners in your enterprise to view IAM data but disallow them to perform any high-risk operations, for example, deleting IAM users and projects. For all permissions of the services supported by IAM, see [System-defined Permissions](#).

## IAM Permissions

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

IAM is a global service deployed for all regions. When you set the authorization scope to **Global services**, users have permission to access IAM in all regions.

You can grant permissions by using roles and policies.

- **Roles:** A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. Cloud services depend on each other. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.
- **Policies:** A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant users only the permissions required to manage ECSs of a certain type. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by IAM, see [Permissions and Supported Actions](#).

[Table 5-1](#) lists all the system-defined permissions for IAM.

**Table 5-1** System-defined permissions for IAM

Role/Policy Name	Description	Type	Content
FullAccess	Full permissions for all services that support policy-based authorization. Users with these permissions can perform operations on all services.	System-defined policy	<a href="#">Content of the FullAccess Policy</a>
IAM ReadOnlyAccess	Read-only permissions for IAM. Users with these permissions can only view IAM data.	System-defined policy	<a href="#">Content of the IAM ReadOnlyAccess Policy</a>
Security Administrator	IAM administrator with full permissions, including permissions to create and delete IAM users.	System-defined role	<a href="#">Content of the Security Administrator Role</a>
Agent Operator	IAM operator (delegated party) with permissions to switch roles and access resources of a delegating party.	System-defined role	<a href="#">Content of the Agent Operator Role</a>
Tenant Guest	Read-only permissions for all services except IAM.	System-defined role	<a href="#">Content of the Tenant Guest Role</a>
Tenant Administrator	Administrator permissions for all services except IAM.	System-defined role	<a href="#">Content of the Tenant Administrator Role</a>

**Table 5-2** lists the common operations supported by system-defined permissions for IAM.

 **NOTE**

**Tenant Guest** and **Tenant Administrator** are basic roles provided by IAM and do not contain any specific permissions for IAM. Therefore, the two roles are not listed in the following table.

**Table 5-2** Common operations supported by system-defined permissions

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Creating IAM users	Supported	Not supported	Supported	Not supported

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Querying IAM user details	Supported	Not supported	Supported	Supported
Modifying IAM user information	Supported	Not supported	Supported	Not supported
Querying security settings of IAM users	Supported	Not supported	Supported	Supported
Modifying security settings of IAM users	Supported	Not supported	Supported	Not supported
Deleting IAM users	Supported	Not supported	Supported	Not supported
Creating user groups	Supported	Not supported	Supported	Not supported
Querying user group details	Supported	Not supported	Supported	Supported
Modifying user group information	Supported	Not supported	Supported	Not supported
Adding users to user groups	Supported	Not supported	Supported	Not supported
Removing users from user groups	Supported	Not supported	Supported	Not supported
Deleting user groups	Supported	Not supported	Supported	Not supported
Assigning permissions to user groups	Supported	Not supported	Supported	Not supported
Removing permissions of user groups	Supported	Not supported	Supported	Not supported

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Creating custom policies	Supported	Not supported	Supported	Not supported
Modifying custom policies	Supported	Not supported	Supported	Not supported
Deleting custom policies	Supported	Not supported	Supported	Not supported
Querying permission details	Supported	Not supported	Supported	Supported
Creating agencies	Supported	Not supported	Supported	Not supported
Querying agencies	Supported	Not supported	Supported	Supported
Modifying agencies	Supported	Not supported	Supported	Not supported
Switching roles	Not supported	Supported	Supported	Not supported
Deleting agencies	Supported	Not supported	Supported	Not supported
Granting permissions to agencies	Supported	Not supported	Supported	Not supported
Removing permissions of agencies	Supported	Not supported	Supported	Not supported
Creating projects	Supported	Not supported	Supported	Not supported
Querying projects	Supported	Not supported	Supported	Supported
Modifying projects	Supported	Not supported	Supported	Not supported
Deleting projects	Supported	Not supported	Supported	Not supported

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Creating identity providers	Supported	Not supported	Supported	Not supported
Importing metadata files	Supported	Not supported	Supported	Not supported
Querying metadata files	Supported	Not supported	Supported	Supported
Querying identity providers	Supported	Not supported	Supported	Supported
Querying protocols	Supported	Not supported	Supported	Supported
Querying mappings	Supported	Not supported	Supported	Supported
Updating identity providers	Supported	Not supported	Supported	Not supported
Updating protocols	Supported	Not supported	Supported	Not supported
Updating mappings	Supported	Not supported	Supported	Not supported
Deleting identity providers	Supported	Not supported	Supported	Not supported
Deleting protocols	Supported	Not supported	Supported	Not supported
Deleting mappings	Supported	Not supported	Supported	Not supported
Querying quotas	Supported	Not supported	Supported	Not supported

Access key management is disabled by default. When **access key management** is enabled, only administrators can manage access keys. If IAM users need to create, enable, disable, or delete their own access keys, they need to ask the administrator to **disable access key management**.

To manage other users' access keys as an IAM user, you must obtain the required permissions. For the required system-defined policies or roles, check **Table 5-3**. For

example, to create an access key for an IAM user, obtain the Security Administrator or FullAccess permission.

**Table 5-3** Access key operations supported by system-defined policies or roles

Operation	Security Administrator	Agent Operator	FullAccess	IAM ReadOnlyAccess
Creating access keys (for other IAM users)	Supported	Not supported	Supported	Not supported
Querying access keys (of other IAM users)	Supported	Not supported	Supported	Supported
Modifying access keys (for other IAM users)	Supported	Not supported	Supported	Not supported
Deleting access keys (for other IAM users)	Supported	Not supported	Supported	Not supported

### Content of the FullAccess Policy

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

### Content of the IAM ReadOnlyAccess Policy

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "iam:*:get*",
        "iam:*:list*",
        "iam:*:check*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## Content of the Security Administrator Role

```
{
  "Version": "1.0",
  "Statement": [
    {
      "Action": [
        "iam:agencies:*",
        "iam:credentials:*",
        "iam:groups:*",
        "iam:identityProviders:*",
        "iam:mfa:*",
        "iam:permissions:*",
        "iam:projects:*",
        "iam:quotas:*",
        "iam:roles:*",
        "iam:users:*",
        "iam:securitypolicies:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## Content of the Agent Operator Role

```
{
  "Version": "1.0",
  "Statement": [
    {
      "Action": [
        "iam:tokens:assume"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## Content of the Tenant Guest Role

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "obs:*:get*",
        "obs:*:list*",
        "obs:*:head*"
      ],
      "Effect": "Allow"
    },
    {
      "Condition": {
        "StringNotEqualsIgnoreCase": {
          "g:ServiceName": [
            "iam"
          ]
        }
      },
      "Action": [
        "obs:*:get*",
        "obs:*:list*",
        "obs:*:head*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

## Content of the Tenant Administrator Role

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "obs:*:*"
      ],
      "Effect": "Allow"
    },
    {
      "Condition": {
        "StringNotEqualsIgnoreCase": {
          "g:ServiceName": [
            "iam"
          ]
        }
      },
      "Action": [
        "*:*:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

# 6 Security

---

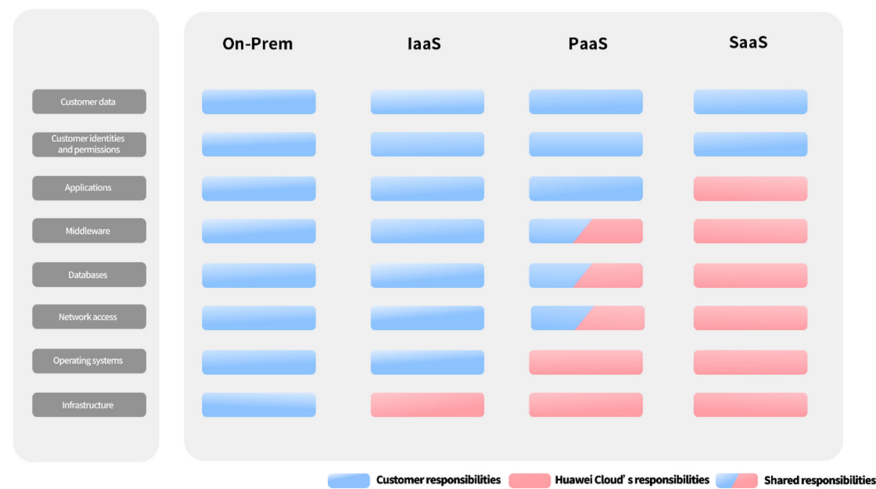
## 6.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in [Figure 6-1](#).

- **Huawei Cloud:** Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer:** As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

**Figure 6-1** Huawei Cloud shared security responsibility model



Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in [Figure 6-1](#), customers can select different cloud service types (such as IaaS, PaaS, and SaaS) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the PaaS middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

**On-premises (On-Prem):** Software and IT infrastructure are deployed and managed by customers within their own data centers, rather than be deployed by remote cloud service providers.

**Infrastructure as a Service (IaaS):** Cloud service providers offer compute, network, storage, and more infrastructure services, including [Elastic Cloud Server \(ECS\)](#), [Virtual Private Network \(VPN\)](#), and [Object Storage Service \(OBS\)](#).

**Platform as a Service (PaaS):** Cloud service providers deliver platforms required for application development and deployment, such as [ModelArts](#) and [GaussDB](#). Customers do not need to maintain the underlying infrastructure.

**Software as a Service (SaaS):** Cloud service providers offer complete application software, such as [Huawei Cloud Meeting](#). Customers use the software directly without the need to install the application, maintain it, or manage its underlying platform or infrastructure.

## 6.2 Authentication and Access Control

### 6.2.1 Identity Authentication

The IAM service requires the access requester to present the identity credential and verifies the identity validity. In addition, the IAM service provides login protection and verification policies to harden the security of identity authentication.

#### Identity Credentials and Their Security

IAM can be accessed using accounts and IAM users. Both of them support identity authentication using usernames, passwords, access keys, and temporary access keys. IAM implements security design for each identity credential to protect user data and enable users to access IAM more securely. For details, see [Table 6-1](#).

**Table 6-1** IAM identity credentials and security design

Access Credential	Security Description	Reference
Username and password	You can configure the character type and minimum length of a user key as required. You can also configure the password validity period policy and minimum password validity period policy.	<a href="#">Password Policy</a>
Access Key	AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.	<a href="#">Access Keys</a>
Temporary Access Key	In addition to the access key feature, a temporary access key has a validity period that can be customized. If the validity period expires, the temporary access key becomes invalid and you have to obtain a new one.	<a href="#">Temporary Access Key (for Federated Users)</a>

## Login Protection and Authentication Policies

As described in [Table 6-2](#), in addition to requiring users to show credentials and verify their validity during login, IAM also provides login protection and supports login authentication policies to prevent user information from being stolen.

**Table 6-2** Login protection and authentication policies

Login Protection Method	Description	Reference
Login Protection	<p>In addition to entering the username and password on the login page (first-time authentication), you need to enter a verification code on the <b>Login Verification</b> page (second-time authentication).</p> <p>Verify that mobile numbers, email addresses, and virtual MFA devices are supported. For details, see <a href="#">MFA Authentication</a>.</p>	<a href="#">Login Protection</a>

Login Protection Method	Description	Reference
Login Authentication Policy	<p>IAM supports the following login authentication policies:</p> <p><b>Session timeout</b> policy: If a user does not log in to the system within a specified period, the user needs to log in again.</p> <p><b>Account lockout</b> policy: If the number of login failures exceeds the threshold, the account is locked.</p> <p><b>Account disabling</b> policy: If a user does not log in to the system for a long time, the account is disabled.</p> <p>Display of <b>recent login information</b>: Users can view the last login time.</p>	<a href="#">Login Authentication Policy</a>

## 6.2.2 Configuring Access Control

IAM uses fine-grained authorization policies and ACLs to control access.

**Table 6-3** IAM access control

Access Policy	Description	Reference
IAM Fine-grained Authorization Policy	<p>IAM service permissions are divided into roles or fine-grained policies. Roles and policies define the user operations allowed or rejected by IAM. For example, if a user or user group has the IAM ReadOnlyAccess permission, the user or user group only has the read-only permission on IAM service data. IAM also supports <b>custom policies</b> to assign IAM service permissions.</p>	<a href="#">IAM Permissions</a>

Access Policy	Description	Reference
ACL	With ACL, you can set access control policies to allow users to log in to the IAM console or open APIs only from specified IP address ranges, network segments, and VPC endpoints.	<a href="#">ACL</a>

## 6.3 Data Protection

### 6.3.1 IAM Side

To ensure that your personal data, such as the username, password, and mobile phone number, will not be obtained by unauthorized or unauthenticated entities or individuals, IAM encrypts your data during storage and transmission to prevent data leakage.

#### Personal Data

[Table 6-4](#) lists the personal data generated or collected by IAM.

**Table 6-4** Personal data

Type	Source	Used For	Modifiable	Mandatory
Username	<ul style="list-style-type: none"> <li>Entered when you create a user on the management console.</li> <li>Entered when you call an API.</li> </ul>	<ul style="list-style-type: none"> <li>User identity identification</li> <li>Identity authentication during console access or API calls</li> </ul>	Yes (Administrators can call the API to change the username.)	Yes Usernames are used to identify users.
Password	<ul style="list-style-type: none"> <li>Entered when you create a user, modify user credentials, or reset the password on the management console.</li> <li>Entered when you call an API.</li> </ul>	Identity authentication during console access or API calls	Yes	No You can also choose AK/SK authentication.

Type	Source	Used For	Modifiable	Mandatory
Email address	Entered when you create a user, modify user credentials, or change the email address on the management console.	<ul style="list-style-type: none"> <li>User identity identification</li> <li>Identity authentication during console access</li> <li>Receiving messages</li> </ul>	Yes	No
Mobile number	Entered when you create a user, modify user credentials, or change the mobile number on the management console.	<ul style="list-style-type: none"> <li>User identity identification</li> <li>Identity authentication during console access</li> <li>Receiving messages</li> </ul>	Yes	No
AK/SK	Displayed in the <b>Security Settings &gt; Access Keys</b> area of a specific user on the IAM console or on the <b>My Credentials &gt; Access Keys</b> page.	Identity authentication during API calls	No AK/SK cannot be modified, but they can be deleted and created again.	No AK/SK are used to sign the requests sent to call APIs.

## Data Storage Security

IAM uses encryption algorithms to encrypt sensitive user data before storing it.

- Usernames and AKs: non-sensitive data, which is stored in plaintext.
- Password: The password is encrypted using the salted SHA512 algorithm.
- Email address, mobile number, and SK: Use the AES algorithm to encrypt and store them.

## Data Transmission Security

Sensitive data (including passwords) of users is encrypted using TLS 1.2 during transmission. All IAM APIs support HTTPS to encrypt data during transmission.

### 6.3.2 Tenant Side

**Shared responsibilities** apply to data protection in Huawei Cloud IAM. As mentioned, IAM is responsible for the security of the service itself and provides a secure data protection mechanism. Tenants are responsible for the secure use of IAM services, including security parameter configuration and permission splitting and granting by enterprises.

For the purpose of data protection, you are advised to use IAM in a more standard manner by referring to [Recommendations for Using IAM](#).

## 6.4 Resilience

Huawei Cloud's data centers are deployed around the world. All data centers are running properly. Data centers in two cities are deployed as disaster recovery center for each other. If a data center in city A is down, the data center in city B automatically takes over the job and serves your applications and data in compliance with the regulations to ensure service continuity. In order to minimize the service interruptions caused by hardware failures, natural disasters, or other disastrous events, Huawei Cloud provides a DR plan for all data centers:

As a basic identity authentication service, Huawei Cloud IAM has been deployed in multiple zones to provide global users with higher availability, fault tolerance, and scalability.

## 6.5 Audit and Monitoring

Cloud Trace Service (CTS) records operations performed on cloud resources in your account. The operation logs can be used to perform security analysis, track resource changes, perform compliance audits, and locate faults.

For details about IAM operations that can be recorded by CTS, see "IAM operations that can be recorded by CTS" in [Key IAM Operations Supported by CTS](#). After you enable CTS and create and configure a tracker, CTS starts to record operations for auditing. For details, see [Key IAM Operations Supported by CTS](#). After CTS is enabled, you can [view CTS traces in the trace list](#). CTS stores operation logs of the last seven days.

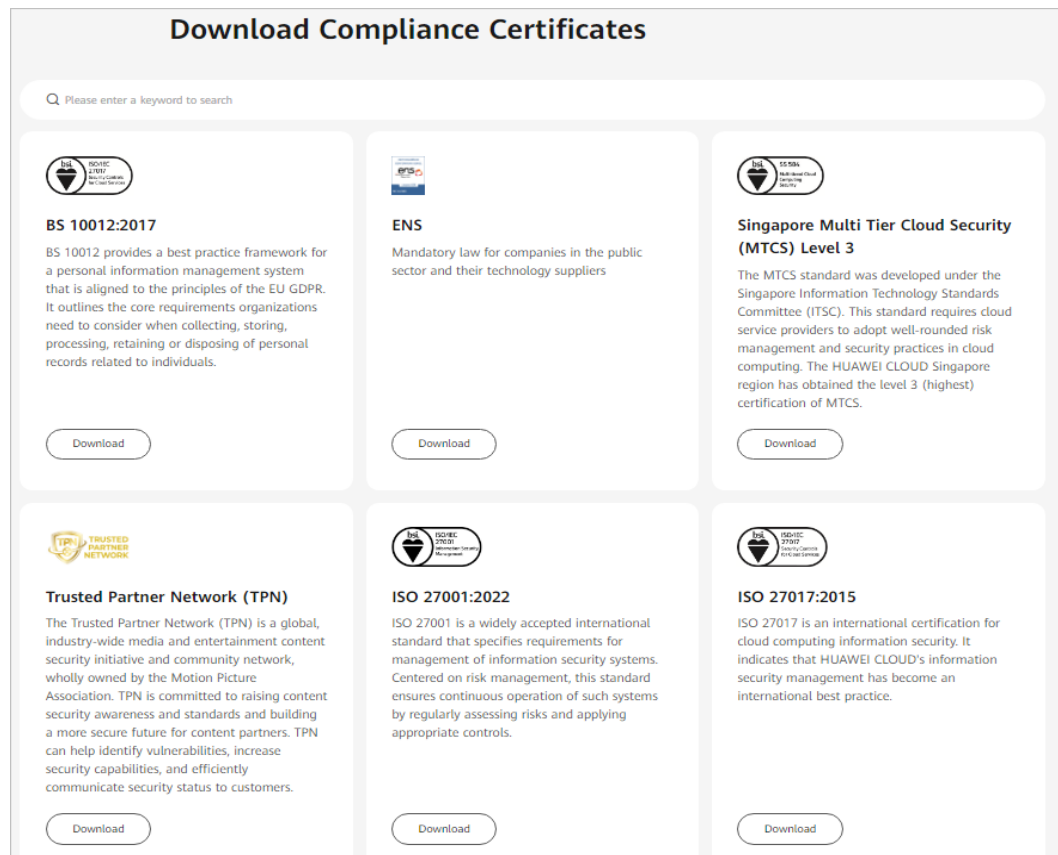
CTS allows you to [create key event notifications](#). You can add IAM-related high-risk and sensitive operations as key operations to the real-time monitoring list of CTS for monitoring and tracing. If a key operation in the monitoring list is triggered when a user uses the IAM service, CTS records the operation log and sends a notification to the related subscriber in real time.

## 6.6 Certificates

### Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can [download](#) them from the console.

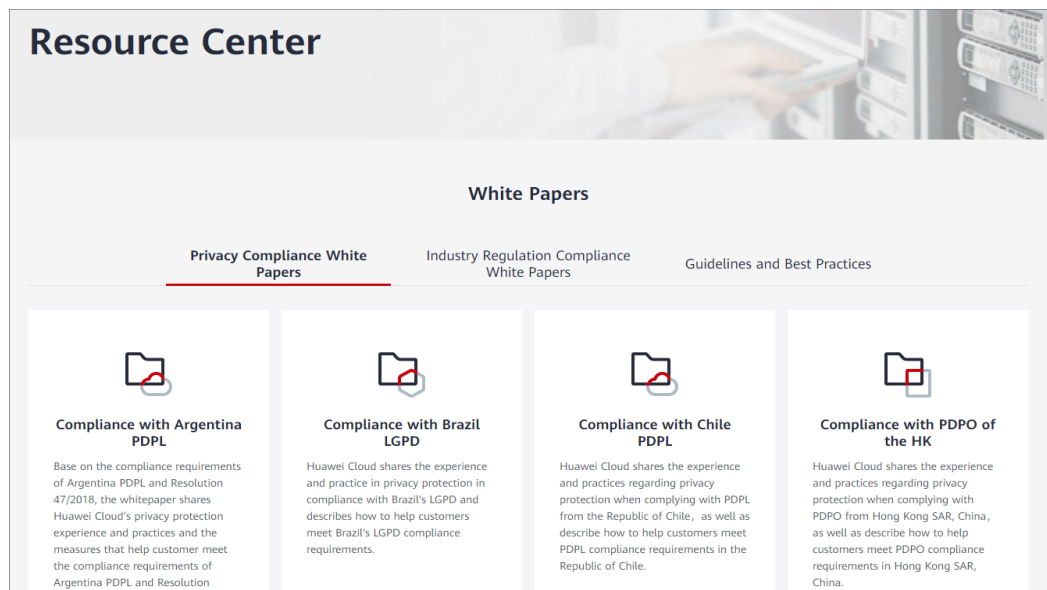
Figure 6-2 Downloading compliance certificates



### Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see [Resource Center](#).

Figure 6-3 Resource center



# 7 Notes and Constraints

This section describes notes and constraints on using IAM.

## Quotas

You can log in to the console and view your default quotas by referring to [How Do I View My Quotas?](#) You can [submit a service ticket](#) to increase your quotas if needed.

**Table 7-1** Quotas

Category	Item	Quota	Adjustable
User	IAM users	50	Yes <a href="#">Submit a service ticket</a> to request for increasing the quota.
	Characters allowed in a username	64	No
	Groups that a user belongs to	10	No
	AK/SK pairs that a user can create	2	No
	Virtual MFA devices that can be associated with a user	1	No

Category	Item	Quota	Adjustable
	Permissions (including system-defined permissions and custom policies) of a user for enterprise projects	500	No
User group	User groups	20	Yes <a href="#">Submit a service ticket</a> to request for increasing the quota.
	Characters allowed in a user group name	128	No
	Users in a user group	IAM users in an account	No
	Permissions (including system-defined permissions and custom policies) of a user group for IAM projects	200	No
	Permissions (including system-defined permissions and custom policies) of a user group for enterprise projects	500	No
Project	Sub-projects in each region	10	Yes <a href="#">Submit a service ticket</a> to request for increasing the quota.
Policy	Characters allowed in a policy name	128	No
Custom policy	Custom policies	200	Yes <a href="#">Submit a service ticket</a> to request for increasing the quota.

Category	Item	Quota	Adjustable
	Characters per policy	6,144	No
	Statements per policy	Unlimited	No
	Actions per statement	Unlimited	No
	Resources per statement	Unlimited	No
	Conditions per statement	Unlimited	No
Agency	Agencies	50	Yes <a href="#">Submit a service ticket</a> to request for increasing the quota.
	Characters allowed in an agency name	64	No
	Permissions (including system-defined permissions and custom policies) of an agency	200	No
Identity provider	Identity providers	10	Yes <a href="#">Submit a service ticket</a> to request for increasing the quota.
	Characters allowed in an identity provider name	64	No
	Mapping rules of all identity providers in an account	10	Yes <a href="#">Submit a service ticket</a> to request for increasing the quota.
	User groups associated with a federated virtual user	100	No

Category	Item	Quota	Adjustable
	Characters allowed in a federated virtual user name	255	No

## Naming Rules

**Table 7-2** Naming rules

Item	Description
Username	<ul style="list-style-type: none"> <li>• A maximum of 64 characters.</li> <li>• Only letters (case-sensitive), digits, spaces, hyphens (-), underscores (_), and periods (.) are allowed. A username cannot start with a digit or space.</li> </ul>
User group name	<ul style="list-style-type: none"> <li>• A maximum of 128 characters.</li> <li>• Only letters (case-sensitive), digits, spaces, hyphens (-), and underscores (_) are allowed.</li> </ul>
Name of a custom policy	<ul style="list-style-type: none"> <li>• A maximum of 128 characters.</li> <li>• Only letters (case-sensitive), digits, spaces, and special characters (-_.,) are allowed.</li> </ul>
Project name	<ul style="list-style-type: none"> <li>• A maximum of 53 characters.</li> <li>• Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.</li> </ul>
Agency name	A maximum of 64 characters.
Identity provider name	<ul style="list-style-type: none"> <li>• A maximum of 64 characters.</li> <li>• Only letters (case-sensitive), digits, hyphens (-), and underscores (_) are allowed.</li> </ul>

## Operation Constraints

**Table 7-3** Operation constraints

Scenario	Item	Description
Creating IAM users	IAM users that can be created at a time	A maximum of 10 users can be created at a time.

Scenario	Item	Description
	IAM username	A new username must be different from existing IAM usernames.
	Mobile number and email address	A mobile number or an email address can be bound only to one account or IAM user.
	IAM user password	An IAM user password cannot be the username or the username spelled backwards. For example, if the username is <b>A12345</b> , the password cannot be <b>A12345</b> , <b>a12345</b> , <b>54321A</b> , or <b>54321a</b> .
Creating custom policies	Policy content	<ul style="list-style-type: none"> <li>• Actions, condition keys, and resource types are all case-insensitive.</li> <li>• If a custom policy contains actions of multiple services, all of them must be global services or project-level services. If you need permissions for both global and project-level services, create two custom policies.</li> </ul>
Creating agencies	Delegated account	The delegated account can only be an account, rather than an IAM user or a federated user.

Scenario	Item	Description
Configuring security settings	Critical operations	<ul style="list-style-type: none"> <li>• An IAM user or account can only bind one device for 2-step verification, which can be a mobile number, an email address or a virtual MFA device.</li> <li>• Before binding a virtual MFA device, ensure that you have installed an MFA application on your device.</li> <li>• Login protection only supports console access for IAM users. It does not support programmatic access.</li> <li>• If your Huawei Cloud account has been upgraded to a HUAWEI ID, login protection cannot be enabled in security settings. To enable login protection, go to <a href="#">Huawei account center</a>, choose <b>Account &amp; security</b>, locate <b>Two-step verification</b> in the <b>Security verification</b> area, and click <b>ENABLE</b>.</li> <li>• The verification is valid for 15 minutes and you do not need to pass verification again when performing critical operations within the validity period.</li> </ul>

Scenario	Item	Description
	Login authentication policy	<ul style="list-style-type: none"> <li>• The account lockout policy applies to both Huawei Cloud accounts and IAM users.</li> <li>• Once locked, accounts or IAM users cannot be unlocked by themselves. The next login is available only after the lock time expires.</li> <li>• The account disabling policy applies only to IAM users. It does not apply to accounts.</li> <li>• The USB key certificate expiration policy applies to both accounts and IAM users.</li> </ul>
	Password policy	<ul style="list-style-type: none"> <li>• If your Huawei Cloud account has been upgraded to a HUAWEI ID, the password policy does not apply to your account (HUAWEI ID).</li> <li>• Only the administrator can configure the password policy. IAM users can only view the policy settings and cannot modify them. If an IAM user needs to modify the settings, the user can request the administrator to do so or grant the required permissions.</li> <li>• The password composition &amp; reuse policy applies to both Huawei Cloud accounts and IAM users.</li> <li>• The password expiration policy is disabled by default.</li> <li>• After the password expires, the newly set password must be different from the old password.</li> <li>• The minimum password age policy is disabled by default. It applies to both accounts and IAM users.</li> </ul>

Scenario	Item	Description
	ACL	<ul style="list-style-type: none"> <li>• A maximum of 200 access control entries can be added.</li> <li>• If an IAM user or a federated user accesses Huawei Cloud through a proxy server, set the allowed IP addresses, address ranges or CIDR blocks based on the proxy IP address. If an IAM user or a federated user accesses Huawei Cloud through a public network, set them based on the public IP address.</li> <li>• Both IPv4 and IPv6 addresses are supported.</li> <li>• Console access (recommended): The ACL policy only applies to console access for IAM users and federated users (SP-initiated). It does not apply to accounts.</li> <li>• API access: The ACL policy only applies to API access through API gateways for IAM users and federated users. The system will apply the settings in 15 minutes.</li> <li>• If you set <b>IP Address Ranges</b>, <b>CIDR Blocks</b>, and <b>VPC Endpoints</b>, you can access using any of them.</li> </ul>
Creating projects	/	<ul style="list-style-type: none"> <li>• If you enable Enterprise Project, IAM projects are not available.</li> <li>• Resources are not transferable across IAM projects.</li> </ul>
Deleting projects	/	<p>Preset projects cannot be deleted.</p> <p>To delete a sub-project, delete it from the project list.</p>

Scenario	Item	Description
Accessing Huawei Cloud as a federated user	Federated user login modes	IAM supports two types of identity federation: <ul style="list-style-type: none"> <li>● Web SSO: Browsers work as the communication media. This authentication type enables common users to access Huawei Cloud using browsers.</li> <li>● API calling: Development tools (such as OpenStackClient and Shibboleth ECP Client) work as the communication media. This authentication type enables enterprise users and common users to access Huawei Cloud by calling APIs.</li> </ul>
	Critical operation protection	Federated users do not need to perform a 2-step verification when performing critical operations even though login protection or operation protection is enabled.
	Permanent access key (AK/SK)	Federated users cannot create access keys with unlimited validity, but they can obtain temporary access credentials (access keys and security tokens) using user or agency tokens. For details, see <a href="#">Obtaining Temporary Access Keys and Security Tokens of an IAM User</a> .