Identity and Access Management

Service Overview

Issue 15

Date 2021-04-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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 What Is IAM?

Huawei Cloud Identity and Access Management (IAM) 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.

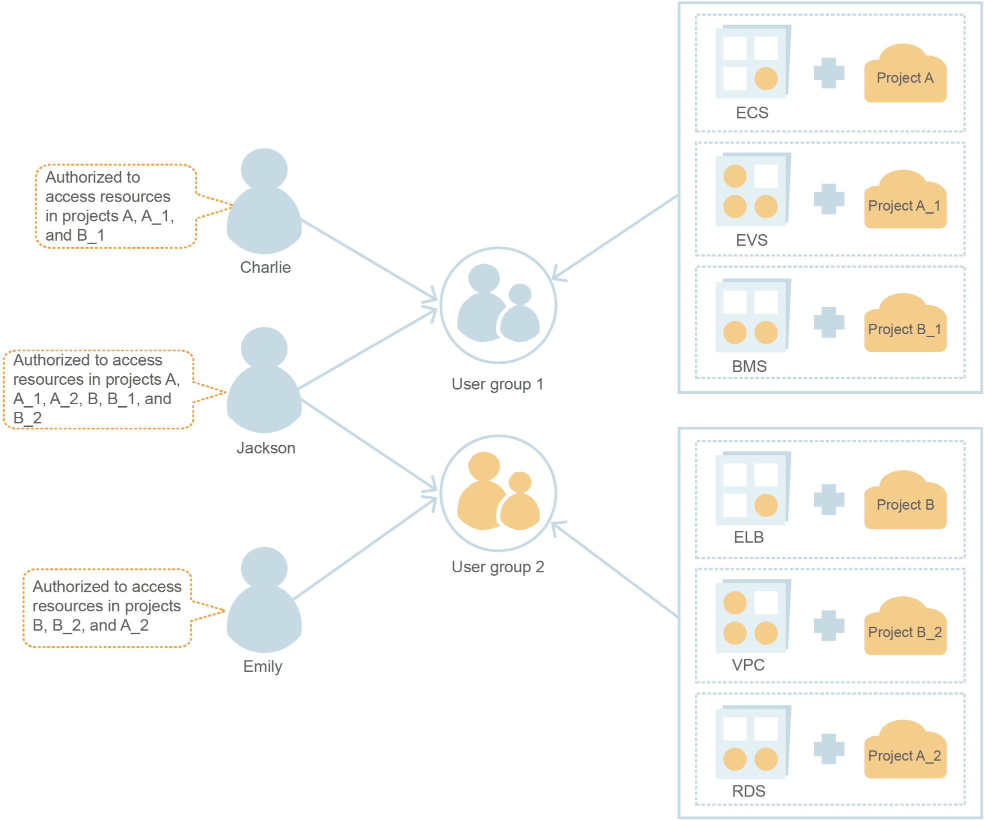
Advantages

Fine-grained access control for Huawei Cloud resources

When you successfully register with Huawei Cloud, your account is automatically created. Your account has full access permissions for your cloud services and resources and makes payments for the use of these resources.

If you purchase multiple Huawei Cloud resources, such as Elastic Cloud Servers (ECSs), Elastic Volume Services (EVSs), 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 and access resources in your account.

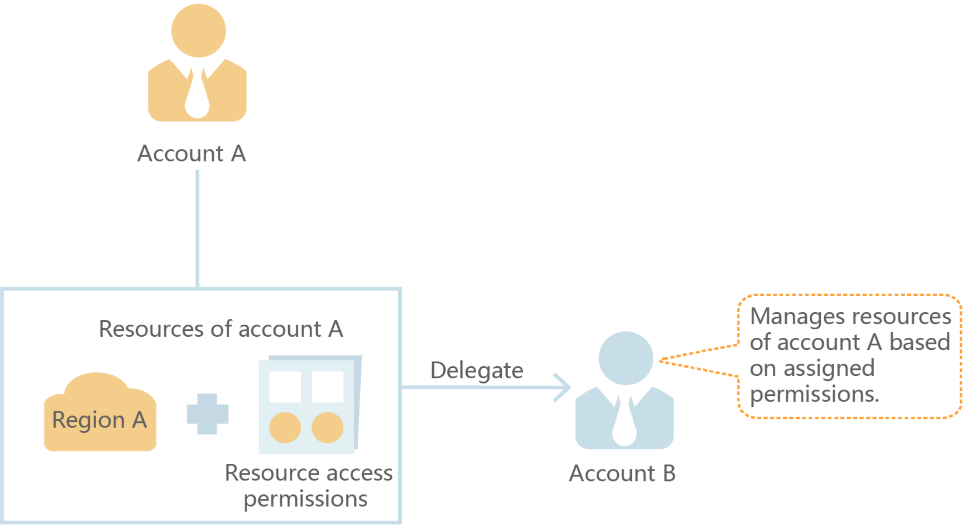
In addition to IAM, you can use Enterprise Management to control access to cloud resources. Enterprise Management supports more fine-grained permissions management and enterprise project management. You can choose either IAM or Enterprise Management to suit your requirements. For details, see **What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


Authorized to access resources in projects A, A_1, and B_1
Charlie
Authorized to access resources in projects A, A_1, A_2, B, B_1, and B_2
Jackson
Authorized to access resources in projects B, B_2, and A_2
Emily
User group 1
User group 2
ECS
Project A
EVS
Project A_1
BMS
Project B_1
ELB
Project B
VPC
Project B_2
RDS
Project A_2

Cross-account resource access delegation

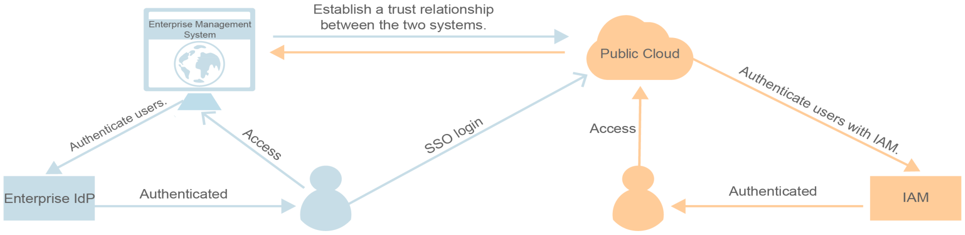
If you purchase multiple Huawei Cloud resources, you can delegate another account to manage some of your resources for efficient O&M.

For example, you can create an agency for a professional O&M company to enable the company to manage specific resources with the company's 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.


Account A
Resources of account A
Region A
Resource access permissions
Delegate
Account B
Manages resources of account A based on assigned permissions.

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 identity provider establishes a trust relationship between your enterprise and Huawei Cloud, allowing the employees to access Huawei Cloud using their existing accounts.


Enterprise Management System
Establish a trust relationship between the two systems.
Public Cloud
Authenticate users.
Access
SSO login
Access
Authenticate users with IAM.
Enterprise IdP
Authenticated
Authenticated
IAM

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 in a programmable way. For details, see **API Reference**.

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 register with Huawei Cloud. Your account has full access permissions for your cloud resources and makes payments for the use of these resources. You can use the account to reset user passwords and assign permissions.

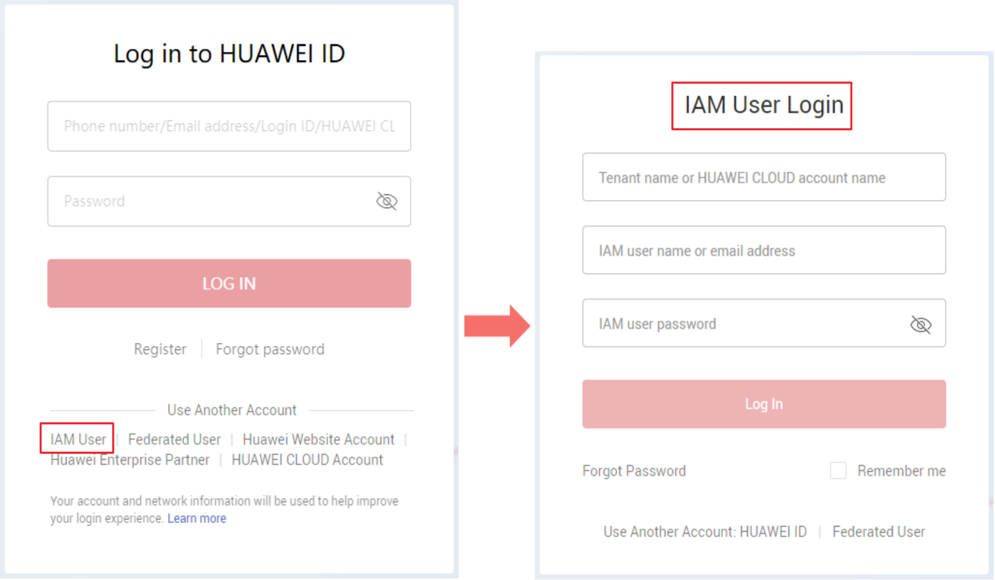
You cannot modify or delete your account in IAM, but you can do so in My Account.

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 (passwords or access keys) and uses cloud resources based on assigned permissions. IAM users cannot make payments themselves. You can use your account to pay their bills.

If an IAM user forgets their password, the user can reset the password by referring to **How Do I Reset My Password?**

Figure 2-1 IAM user login

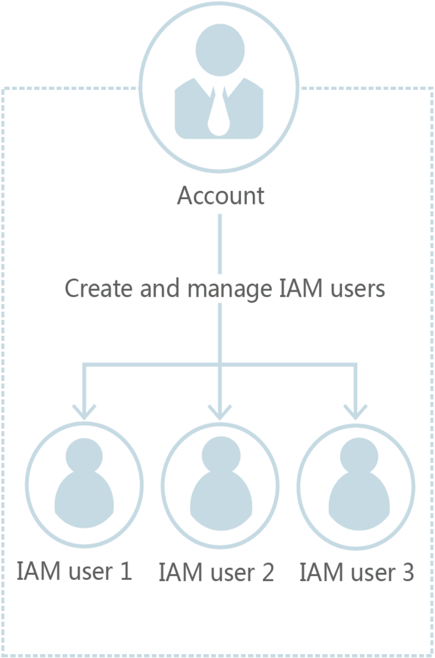

Log in to HUAWEI ID
Phone number/Email address/Login ID/HUAWEI CL
Password
LOG IN
Register | Forgot password
Use Another Account
IAM User | Federated User | Huawei Website Account |
Huawei Enterprise Partner | HUAWEI CLOUD Account
IAM User Login
Tenant name or HUAWEI CLOUD account name
IAM user name or email address
IAM user password
Log In
Forgot Password
Remember me
Use Another Account: HUAWEI ID | Federated User

Your account and network information will be used to help improve your login experience. Learn more

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 makes payments 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.

Figure 2-2 Account and IAM users



Authorization

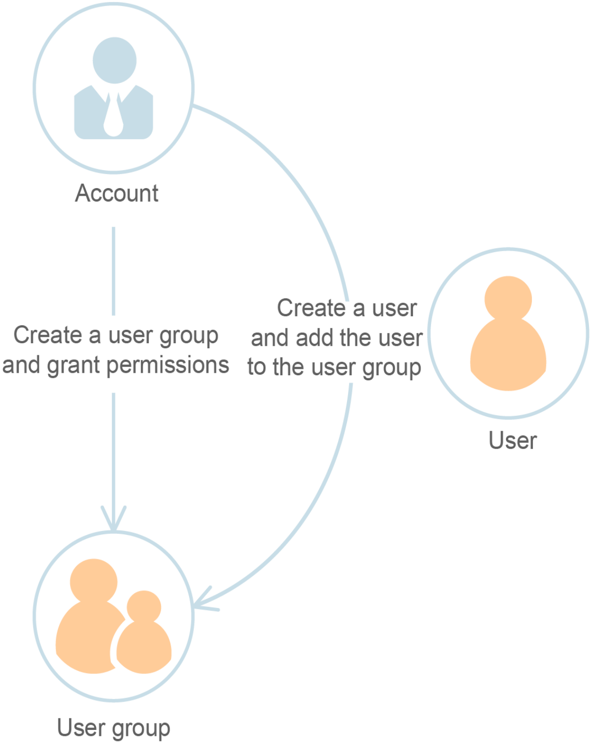
Authorization is the process of granting required permissions for a user to perform specific tasks.

User Group

An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users, which can make it easier to manage the permissions for those users. IAM users added to a user group automatically obtain the permissions assigned to 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


Account
Create a user group and grant permissions
Create a user and add the user to the user group
User
User group

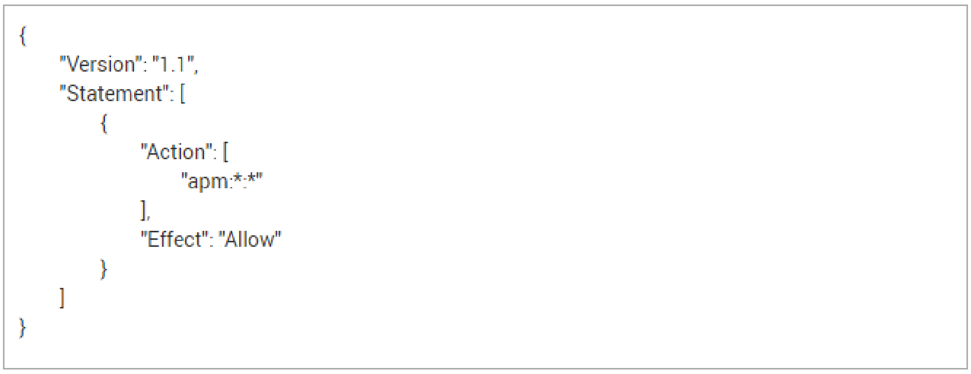
Permissions

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 permission 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. System-defined policies can be used to assign permissions to user groups, and cannot be modified. 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, it indicates that 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

Credentials confirm the identity of a user when the user accesses Huawei Cloud through the console or APIs. Credentials can be either a password 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, which can only be used to call APIs. Each access key provides a signature for cryptographic authentication to ensure that access requests are secret, complete, and correct.

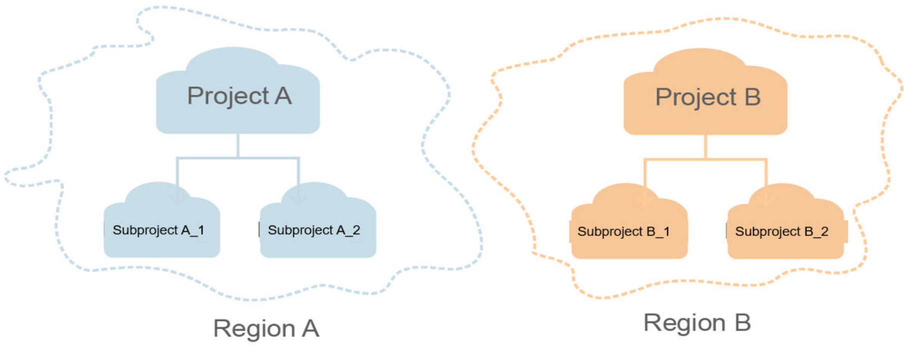
Virtual MFA Device

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 resources (including computing, 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

A trust relationship that you can establish between your account and another account or a cloud service to delegate resource access.

- 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.

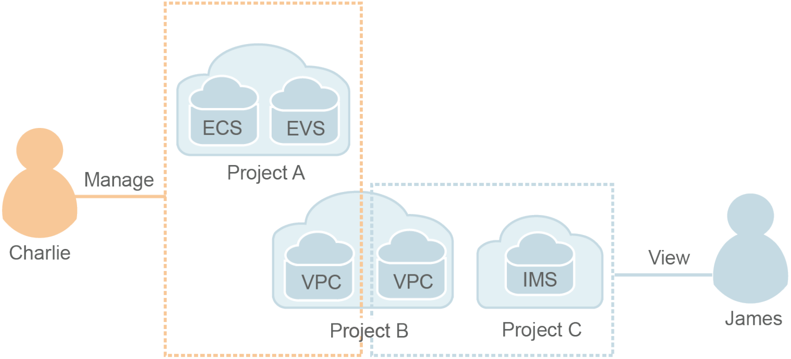
3 Functions

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



Secure Access

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

Critical Operation Protection

IAM provides login protection and critical operation protection, making your account and resources more secure. When you or users created using your account log in to the console or perform a critical operation, you and the users need to complete authentication by email, SMS, or virtual MFA device.

User Group–based Permissions Assignment

With IAM, you do not need to assign permissions to single users. Instead, you can manage users by group and assign permissions to the specified group. Each user then inherits permissions from their groups. To change the permissions of a user, you can remove the user from the original groups or add the user to other groups.

Project-based Resource Isolation

You can create subprojects in a region so that resources in that region can be isolated from each other.

Federated Identity Authentication

Enterprises with identity authentication systems can access Huawei Cloud through single sign-on (SSO), eliminating the need to create users on Huawei Cloud.

Resource Management Delegation

You can delegate more professional, efficient accounts or other cloud services to manage specific resources in your account.

Account Security Settings

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

Eventual Consistency

Results of your IAM operations, such as creating users and user groups and assigning permissions, may not take effect immediately because data is replicated across different servers in Huawei Cloud's data centers around the world. Ensure that the operation results have taken effect before you perform any other operations that depend on them.

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 lists the IAM-supported services and table heading descriptions.

- 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 called global services. Permissions for these services must be assigned in global regions. Users do not need to switch regions when they access these services.
  - Specific regions: Services deployed for specific regions are called project-level services. Permissions for these services need to be assigned in specific regions and take effect only for the corresponding 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.
- Agency: Whether a service can be delegated 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 defining the operations that can be performed 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	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	Agency	Policy	Enterprise Project
Elastic Volume Service (EVS)	Specific regions	√	√	x	√	√
Storage Disaster Recovery Service (SDRS)	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	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	Agency	Policy	Enterprise Project
Virtual Private Cloud (VPC)	Specific regions	√	√	x	√	√
Elastic Load Balance (ELB)	Specific regions	√	√	x	√	√
Domain Name Service (DNS)	Global regions	√	√	x	x	√
NAT Gateway	Specific regions	√	√	x	√	√
Direct Connect	Specific regions	√	x	x	x	x
Virtual Private Network (VPN)	Specific regions	√	x	x	√	x
Cloud Connect (CC)	Specific regions	√	x	x	√	√
VPC Endpoint (VPCEP)	Specific regions	√	√	x	x	x

Containers

Service	Scope	Console	API	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	Agency	Policy	Enterprise Project
Relational Database Service (RDS)	Specific regions	√	√	x	√	√
Document Database Service (DDS)	Specific regions	√	x	x	√	√
Distributed Database Middleware (DDM)	Specific regions	√	√	x	√	√
Data Replication Service (DRS)	Specific regions	√	√	x	√	√
Data Admin Service (DAS)	Specific regions	√	x	x	x	x
GaussDB NoSQL	Specific regions	√	√	x	√	√

Security & Compliance

Service	Scope	Console	API	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
Data Encryption Workshop (DEW)	Specific regions	√	√	x	x	x
Managed Detection and Response (MDR)	Specific regions	√	x	x	x	x
SSL Certificate Manager (SCM)	Global regions	√	√	x	√	x
Container Guard Service (CGS)	Specific regions	√	x	x	√	x
Situation Awareness (SA)	Global regions	√	√	√	√	x
Cloud Bastion Host (CBH)	Specific regions	√	√	x	√	x
Data Security Center (DSC)	Specific regions	√	√	x	√	x

Management & Governance

Service	Scope	Console	API	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	√	√
Tag Management Service (TMS)	Global regions	√	√	x	x	x

Application

Service	Scope	Console	API	Agency	Policy	Enterprise Project
ServiceStage	Specific regions	√	√	x	x	x
Distributed Cache Service (DCS)	Specific regions	√	√	x	√	√
Distributed Message Service (DMS)	Specific regions	√	√	√	√	√

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

DeC

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

Migration

Service	Scope	Console	API	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	Agency	Policy	Enterprise Project
Intelligent EdgeCloud (IEC)	Global regions	√	x	x	√	x

EI

Service	Scope	Console	API	Agency	Fine-Grained Policy	Enterprise Project
ModelArts	Specific regions	√	√	√	√	√
Data Lake Governance Center (DGC)	Specific regions	√	√	√	√	x
MapReduce Service (MRS)	Specific regions	√	√	x	√	√
Data Warehouse Service (DWS)	Specific regions	√	√	√	√	√
CloudTable	Specific regions	√	√	x	x	√

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

Enterprise Applications

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

Cloud Communications

Service	Scope	Console	API	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	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	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	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
Enterprise Project Management Service (EPS)	Global regions	√	√	x	√	x
Service Tickets	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	Agency	Policy	Enterprise Project
Message Center	Specific regions	√	x	x	√	x

5 Permissions

If you need to assign different permissions for IAM to employees in your organization, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your Huawei Cloud resources.

With IAM, you can create IAM users under your account, and assign permissions to these users to control their access to 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 the permissions they have been assigned.

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 permission 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	**Content of the FullAccess Policy**
IAM ReadOnlyAccess	Read-only permissions for IAM. Users with these permissions can only view IAM data.	System-defined policy	**Content of the IAM ReadOnlyAccess Policy**
Security Administrator	IAM administrator with full permissions, including permissions to create and delete IAM users.	System-defined role	**Content of the Security Administrator Role**
Agent Operator	IAM operator (delegated party) with permissions to switch roles and access resources of a delegating party.	System-defined role	**Content of the Agent Operator Role**
Tenant Guest	Read-only permissions for all services except IAM.	System-defined policy	**Content of the Tenant Guest Role**
Tenant Administrator	Administrator permissions for all services except IAM.	System-defined policy	**Content of the Tenant Administrator Role**

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**.

If an IAM user wants to manage the access keys of other IAM users, see **Table 3**. For example, if IAM user A wants to create an access key for IAM user B, IAM user A must have 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": [
                "*:*:get*",
                "*:*:list*",
                "*:*: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

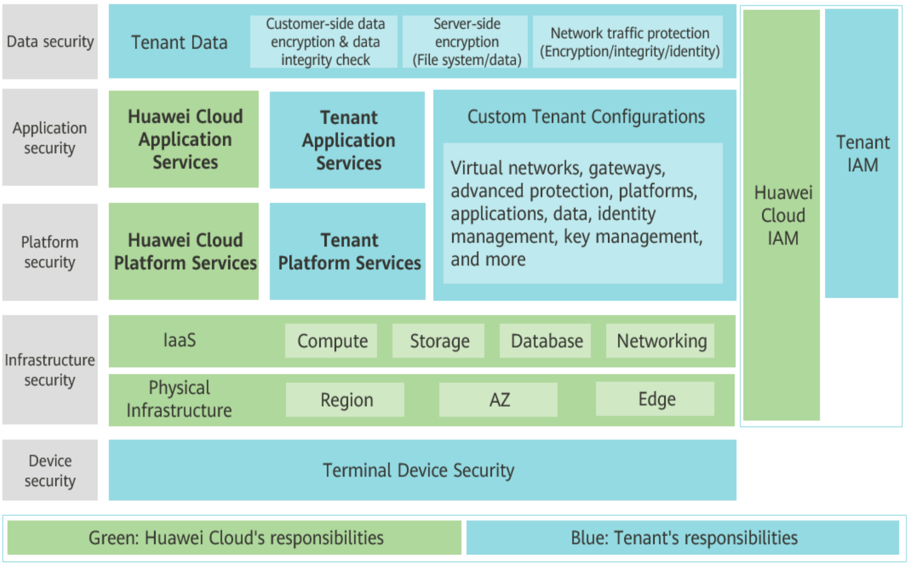
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system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

Figure 6-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 6-1 Huawei Cloud shared security responsibility model


Data security
Tenant Data
Customer-side data encryption & data integrity check
Server-side encryption (File system/data)
Network traffic protection (Encryption/integrity/identity)
Application security
Huawei Cloud Application Services
Tenant Application Services
Custom Tenant Configurations
Virtual networks, gateways, advanced protection, platforms, applications, data, identity management, key management, and more
Platform security
Huawei Cloud Platform Services
Tenant Platform Services
Infrastructure security
IaaS
Compute
Storage
Database
Networking
Physical Infrastructure
Region
AZ
Edge
Device security
Terminal Device Security
Huawei Cloud IAM
Tenant IAM
Green: Huawei Cloud's responsibilities
Blue: Tenant's responsibilities

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.	**Password Policy**
Access Key	AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct.	**Access Keys**
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.	**Temporary Access Key (for Federated Users)**

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 verification policies to prevent user information from being stolen.

Table 6-2 Login protection and authentication policies

Login Protection Method	Description	Functions
Login Protection	In addition to entering the username and password on the login page (first-time authentication), you need to enter a verification code on the **Login Verification** page (second-time authentication). Verify that mobile numbers, email addresses, and virtual MFA devices are supported. For details, see **MFA Authentication**.	**Login Protection**
Login Authentication Policy	IAM supports the following login authentication policies: **Session timeout** policy: If a user does not log in to the system within a specified period, the user needs to log in again. **Account lockout** policy: If the number of login failures exceeds the threshold, the account is locked. **Account disabling** policy: If a user does not log in to the system for a long time, the account is disabled. Display of **recent login information**: Allows users to view the last login time.	**Login Authentication Policy**

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	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 **custom policies** to assign IAM service permissions.	**IAM Permissions**
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.	**ACL**

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.	• Entered when you create a user on the management console. • Entered when you call an API.	• User identity identification • Identity authentication during console access or API calling	Yes (Administrators can call the API to change the username.)	Yes Usernames are used to identify users.
Password	• Entered when you create a user, modify user credentials, or reset the password on the management console. • Entered when you call an API.	Identity authentication during console access or API calling	Yes	No You can also choose AK/SK authentication.
Email address	Entered when you create a user, modify user credentials, or change the email address on the management console.	• User identity identification • Identity authentication during console access • Receiving messages	Yes	No
Mobile number	Entered when you create a user, modify user credentials, or change the mobile number on the management console.	• User identity identification • Identity authentication during console access • Receiving messages	Yes	No

Type	Source	Used For	Modifiable	Mandatory
AK/SK	Displayed in the **Security Settings** > **Access Keys** area of a specific user on the IAM console or on the **My Credentials** > **Access Keys** page.	Identity authentication during API calling	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 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 **Enabling CTS**. After you enable CTS and create and configure a tracker, CTS starts to record operations for auditing. For details, see **Enabling CTS**. After CTS is enabled, you can **view IAM audit logs**. CTS stores operation logs of the last seven days.

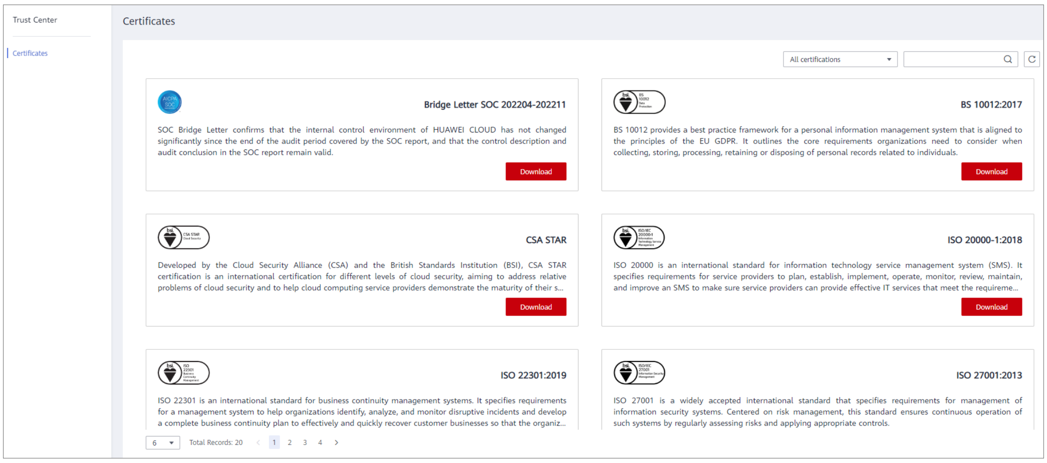
CTS allows you to **configure key event notifications**. You can add IAM-related high-risk and sensitive operations as key operations to the real-time monitoring list of CTS for monitoring and tracing. If a key operation in the monitoring list is triggered when a user uses the IAM service, CTS records 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



Bridge Letter SOC 202204-202211

SOC Bridge Letter confirms that the internal control environment of HUAWEI CLOUD has not changed significantly since the end of the audit period covered by the SOC report, and that the control description and audit conclusion in the SOC report remain valid.

Download

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

Download

CSA STAR

Developed by the Cloud Security Alliance (CSA) and the British Standards Institution (BSI), CSA STAR certification is an international certification for different levels of cloud security, aiming to address relative problems of cloud security and to help cloud computing service providers demonstrate the maturity of their s...

Download

ISO 20000-1:2018

ISO 20000 is an international standard for information technology service management system (SMS). It specifies requirements for service providers to plan, establish, implement, operate, monitor, review, maintain, and improve an SMS to make sure service providers can provide effective IT services that meet the requireme...

Download

ISO 22301:2019

ISO 22301 is an international standard for business continuity management systems. It specifies requirements for a management system to help organizations identify, analyze, and monitor disruptive incidents and develop a complete business continuity plan to effectively and quickly recover customer businesses so that the organiz...

ISO 27001:2013

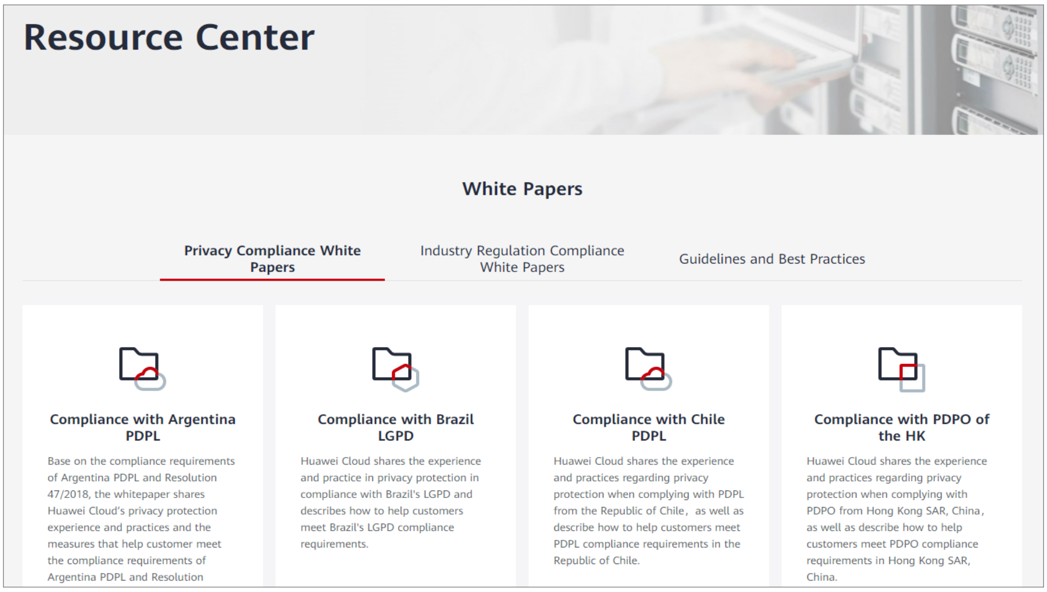
ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

6 Total Records: 20 < 1 2 3 4 >

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



Resource Center

White Papers

Privacy Compliance White Papers

Industry Regulation Compliance White Papers

Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile， as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China， as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

7 Notes and Constraints

The following table lists the quotas of various resources on IAM. For details, see **How Do I Increase My Quota?**

Category	Item	Quota	Adjustable
User	IAM users	50	Yes
	Characters allowed in a username	32	No
	Groups to which a user can be added	10	No
	AK/SK pairs that a user can create	2	No
	Virtual MFA devices that can be associated with a user	1	No
	Permissions (including system-defined permissions and custom policies) that can be assigned to a user for enterprise projects	500	Yes
User group	User groups	20	Yes
	Characters allowed in a user group name	64	No

Category	Item	Quota	Adjustable
	Users that can be added to a user group	IAM users who have been created using your account	No
	Permissions (including system-defined permissions and custom policies) that can be assigned to a user group for IAM projects	200	Yes
	Permissions (including system-defined permissions and custom policies) that can be assigned to a user group for enterprise projects	500	Yes
Project	Subprojects in each region	10	Yes
Policy	Characters allowed in a policy name	64	No
Custom policy	Custom policies	200	Yes
	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
	Characters allowed in an agency name	64	No

Category	Item	Quota	Adjustable
	Permissions (including system-defined permissions and custom policies) that can be assigned to an agency	200	Yes
Identity provider	Quantity	10	Yes
	Characters that can be contained in an identity provider name	64	No
	Mapping rules of all identity providers in an account	10	Yes

8 Change History

Table 8-1 Change history

Date	Description
2022-11-10	This issue is the eighteenth official release, which incorporates the following change: Added introduction to IAM security features in **Security**.
2021-12-01	This issue is the seventeenth official release, which incorporates the following change: Added the identity conversion rule quota in **Notes and Constraints**.
2021-11-23	This issue is the sixteenth official release, which incorporates the following change: Added the description of enterprise projects in **Supported Cloud Services**.
2021-04-25	This issue is the fifteenth official release, which incorporates the following change: Added permission quotas in **Notes and Constraints**.
2020-12-30	This issue is the fourteenth official release, which incorporates the following change: Updated the screenshots in **Basic Concepts** based on the change to the login method.
2020-11-30	This issue is the thirteenth official release, which incorporates the following change: Updated the description based on changes on the security setting page.
2020-10-27	This issue is the twelfth official release, which incorporates the following change: Updated the screenshots in **Basic Concepts** based on the change to the login method.

Date	Description
2020-09-30	This issue is the eleventh official release, which incorporates the following change: Added section **Permissions**.
2020-06-11	This issue is the tenth official release, which incorporates the following change: Changed the maximum number of user groups to which a user can be added to **10** in **Notes and Constraints**.
2020-06-08	This issue is the ninth official release, which incorporates the following change: Added descriptions about HUAWEI ID in **Basic Concepts** and updated the screenshots of the login page.
2020-01-19	This issue is the eighth official release, which incorporates the following changes: ● Optimized the description of permissions in **Basic Concepts**. ● Added the limit of subprojects in a region in **Notes and Constraints**.
2019-11-20	This issue is the seventh official release, which incorporates the following change: Increased the custom policy quota to 200 in **Notes and Constraints**.
2019-06-05	This issue is the sixth official release. Modified descriptions in chapters **What Is IAM?**, **Basic Concepts**, and **Functions**.
2019-03-05	This issue is the fifth official release. Added chapter **Notes and Constraints**.
2019-02-20	This issue is the fourth official release. Added chapter **Basic Concepts**.
2019-01-15	This issue is the third official release. Added chapter **Supported Cloud Services**.
2018-08-10	This issue is the second official release, which incorporates the following change: Added "Personal Data Protection".
2018-03-30	This issue is the first official release.