# IAM 5.0 Service Overview

**Issue** 01

**Date** 2025-11-06

HUAWEI

**HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.**

### Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

### Notice

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

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

## Huawei Cloud Computing Technologies Co., Ltd.

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

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

# Contents



# 1 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.

NOTE

The new IAM console is being rolled out progressively at the account level. If you do not yet have access to the new IAM console, you can enable the Organizations service and Resource Access Manager (RAM) service to start managing identity policy permissions on the new IAM console. This document is the new version of the IAM documentation corresponding to the new IAM console. Unless otherwise specified, the IAM console mentioned in this document refers to the new IAM console. For more information about the differences between the old and new consoles, see **6 Differences Between the Old and New IAM Consoles**.

## Advantages

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

When you successfully sign up for Huawei Cloud, your account is automatically created. This account serves as the owner of resources and the entity responsible for billing usage. The account root user has full access permissions for your cloud services and resources and is able to access all Huawei Cloud services.

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 IAM users enable fine-grained permission control when multiple users collaborate on the same account.

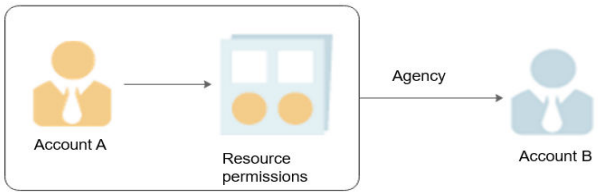
**Cross-account resource access delegation**

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

For example, if you want a professional managed service provider (MSP) to help you manage resources, you can use the trust agency function of IAM to delegate

the resources to the MSP. You can modify or cancel the trust agency anytime. In the following figure, account A is the delegating party, and account B is the delegated party.




## 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

This chapter describes the basic concepts used in 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. The account root user has full access permissions for your cloud services and resources. You can use the account root user 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 your account in IAM, but you can do so in My Account. You can also delete your account in My Account.

NOTE

An account is identified by an account name and an account ID. In IAM or other cloud service documents, "domain name" and "domain ID" refer to the same things. The account name equals the domain name, and the account ID equals the domain ID.

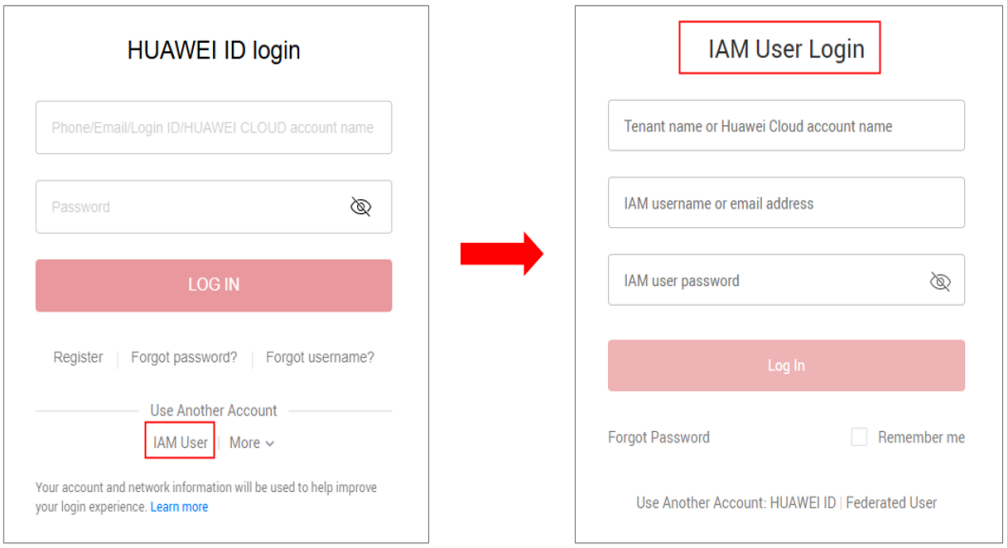
## IAM User

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 permissions assigned by administrators. 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 **What Should I Do If I Forgot My Password?**

**Figure 2-1** IAM user login




## Account Root User

When you create an account, an account root user with the same name as the account is created by default.

Conceptually, the account root user is also an IAM user and has the same capabilities as an IAM user.

However, there are some use constraints on the account root user.

**Constraint 1: The account root user has default authorizations.**

The account root user has default full access to all resources in the account and can assign permissions to IAM users.

**Constraint 2: The permissions of the account root user cannot be changed.**

You cannot grant permissions to or revoke permissions from the account root user, or add the user to or remove it from a user group.

**Constraint 3: The account root user cannot be deleted.**

The account root user cannot be deleted. This ensures that there is at least one IAM user for you to fully control the resources in the account.

NOTE

- We strongly recommend that you do not use the account root user for your daily tasks.
- You need to protect the account root user credentials from being leaked.

## Relationship Between an Account and Its IAM Users

**Conceptual models**

- Account: An account is the entity that owns and pays for used resources. An account does not directly use resources.

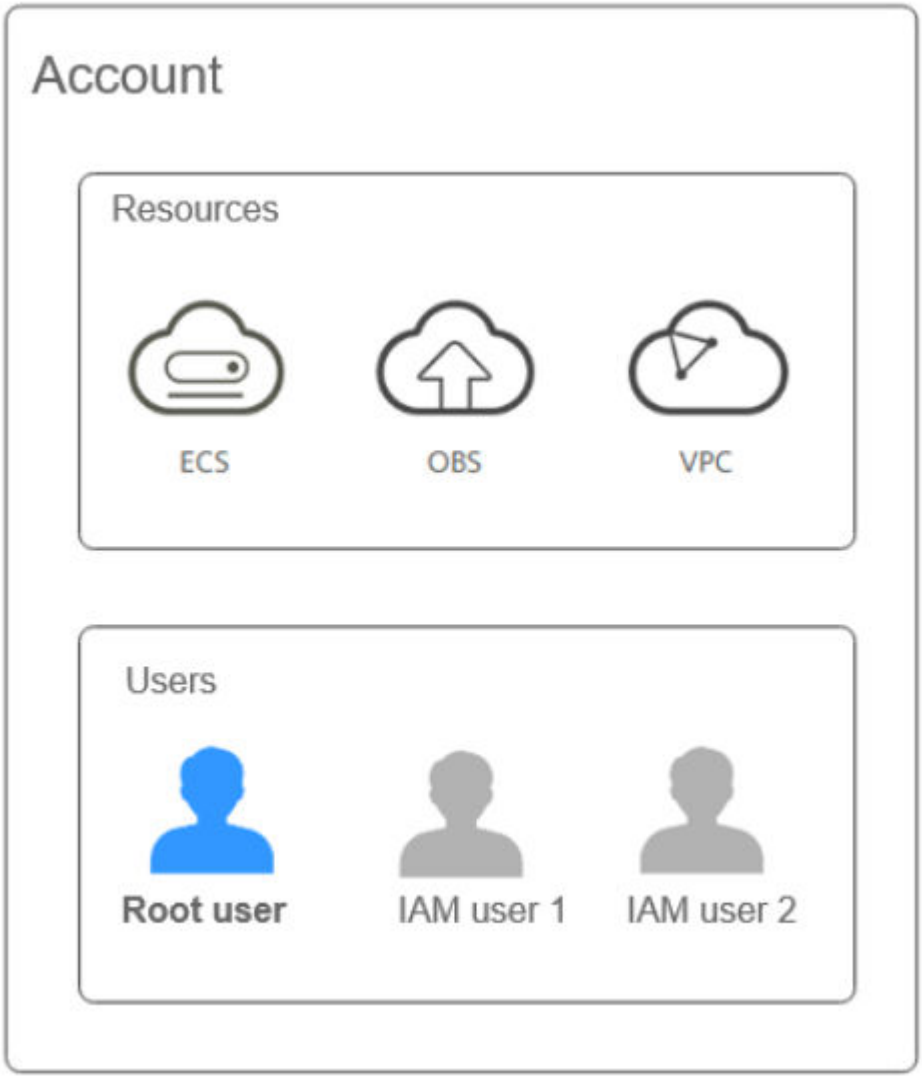
  

- IAM user: IAM users are entities that use resources in an account.

**Usage habits**

There are an account root user and IAM users in an account.

- Account root user: An account root user is an IAM user with the same name as the account. It is created by default when an account is created. There are some **restrictions on account root users**.
- IAM user: An IAM user is manually created after an account is created. IAM users can be modified and deleted.




## User Group

An IAM user group is a collection of IAM users. User groups let you specify permissions for multiple users in batches, making 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 cloud services and 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 2-2** User group and users


## Trust Agency

A trust agency is an IAM identity with specific permissions that you can create in your account. Like IAM users, trust agencies can be bound to identity policies. Identity policies determine what an identity can and cannot do on Huawei Cloud. However, a trust agency is not attached to only one user. Instead, it can be used by anyone who needs it. Unlike IAM users, trust agencies do not have long-term credentials (such as passwords or permanent access keys) associated with them. When you switch to a trust agency, the trust agency provides temporary security credentials for your assumed-trust agency session. A trust relationship can be established between your account and another account or a cloud service.

- Account delegation: You can delegate a third-party account to implement O&M on your resources based on assigned permissions.
- Cloud service delegation: You can create a trust agency to delegate a cloud service to perform O&M on your resources.

Among them, a special type of cloud service trust agency is called a service-linked agency, which is created by the cloud service on your behalf. You can manage the permissions of a cloud service trust agency, but not a service-linked agency. Service-linked agencies are managed by cloud services. For more information, see **Trust Agencies Overview**.

On the **Agencies** page of the new IAM console, both agencies and trust agencies are displayed. For details about the differences between them, see the **Trust Policy** section. In the new IAM documentation, there are agencies and trust agencies. Both allow you to delegate resource management to others. In IAM

documentation, we use the word "agencies" to refer to the non-trust agencies in IAM.

## IAM Identity

IAM identities are IAM resources that you can attach identity policies to. They include IAM users, user groups, agencies, and trust agencies.

## IAM Principal

A principal is an entity that can request operations on resources. It includes IAM users, agencies, and trust agencies. A principal must be authenticated when accessing APIs. A principal is also a resource, so the principal URN must comply with the resource URN format.

## Identity Policy

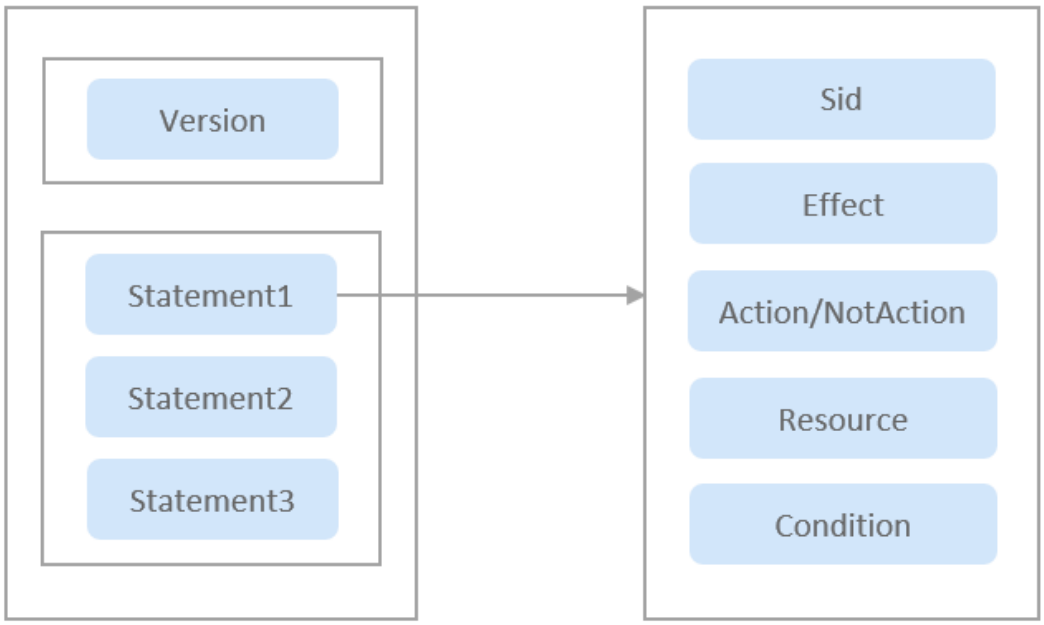
Identity policies define permissions for actions on resources. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant IAM users only permissions to manage ECSs of a certain type. IAM supports both system-defined identity policies and custom identity policies.

- System-defined identity policies define the common actions on cloud services. These policies cannot be modified and can only be used to assign permissions to user groups. If you cannot find system-defined identity policies for a specific cloud service in IAM when you are trying to assign permissions to users, user groups, or trust agencies, it means the cloud service does not support IAM so far. In this case, you can **submit a service ticket** to request the identity policies to be predefined in IAM.
- You can also create **custom identity policies** using the actions supported by cloud services and attach the policies to users, user groups, agencies, and trust agencies. You can create custom identity policies in the visual editor or in JSON view.

**Figure 2-3** shows the structure of an identity policy. An identity policy consists of a version and one or more statements (used for different permissions control). The version of an identity policy is 5.0. In a statement, **Sid** indicates the statement ID, and **Effect** can be **Allow** or **Deny**, which respectively indicate that the action is allowed or denied. The Action/NotAction is in the format of {service name}:{resource type}:{action name}. A resource URN is in the format of {service name}:{region id}:{account id}:{resource type}:{resource name}. Condition supports six types of condition operators: String, Number, Date, Bool, IP Address, and Null. Identity policies also provide more than 40 global condition keys for more flexible and secure access control. For details about the elements in an identity policy, see **JSON Element Reference**.

**Figure 2-3** Structure of an identity policy




The following example describes the structure of an identity policy.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "kms:cmk:decryptData"
      ],
      "Resource": [
         "*"
      ],
      "Condition": {
         "StringNotEquals": {
            "g:ResourceAccount": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
         }
      }
   }]
}
```

This example identity policy ensures that users can use the KMS keys of only the specified users to decrypt data. For details about identity policies, see **Syntax of an Identity Policy**. For more examples, see **Example Custom Identity Policies**. IAM identity policies define more standard and fine-grained actions and support more global condition keys, while policies only support eight global condition keys. If you need to use policy-based authorization, see **Permissions Management**.

## Authorization

Authorization is the process of granting permissions to IAM identities (users, user groups, agencies, and trust agencies) so that the principals (users, agencies, and trust agencies) can access resources on Huawei Cloud. Authorization defines the relationship between IAM identities and permissions. When authorizing IAM identities, the security administrator can directly attach system-defined or custom identity policies to users, user groups, agencies, and trust agencies. Different from the role/policy-based authorization model, there is no need to specify the authorization scope. You can directly attach identity policies to IAM identities.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Allow",
      "Action": ["ecs:*:*"],
      "Resource": ["*"],
      "Condition": {
         "StringEquals": {
            "g:RequestedRegion": "cn-north-4"
         }
      }
   }]
}
```

If you want to control the authorization scope as you do with identity policy-based authorization, you can use the **g:RequestedRegion** condition key. For example, if the preceding identity policy is directly attached to IAM users, IAM users are only allowed to access ECS resources in the cn-north-4 region. If you need to use role/policy-based authorization, see **Permissions Management**. Due to compatibility issues, system-defined and custom identity policies can be attached to agencies on the new IAM console, but system-defined roles and policies as well as custom policies cannot be attached to trust agencies on the old IAM console. You are advised not to use the agencies and identity policies together or trust agencies and roles/policies together.

## Credentials

Credentials confirm the principal of a user when the user accesses Huawei Cloud through the console or APIs. Credentials include passwords, access keys, and temporary security credentials. You can manage the credentials of principals (IAM users, agencies, and trust agencies) in IAM.

| Credentials | Principal | Security | Reference |
| --- | --- | --- | --- |
| Username and password | IAM user | You can configure the character type and minimum length of a user password as required. You can also configure the password validity period policy and minimum password validity period policy. | **Password Policy** |
| Access key | IAM user | Huawei Cloud uses AK together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct. | **Access Keys** |

| Credentials | Principal | Security | Reference |
| --- | --- | --- | --- |
| Temporary security credential | Agency or trust agency | 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 Security Credentials** |

## MFA

Multi-factor authentication (MFA) adds an extra layer of protection on top of your username and password. After MFA authentication is enabled, you need to enter verification codes after your username and password are authenticated. MFA devices, together with your username and password, ensure the security of your account and resources.

## URN

A uniform resource name (URN) that is used to uniquely identify a cloud service resource.

A URN is in the following format: <service-name>:<region>:<account-id>:<type-name>:<resource-path>

- **service-name**: the abbreviation of a cloud service name, for example, **ecs**.
- **region**: the region where the resource is located, for example, **cn-north-1**. If the resource is a global service resource, leave this field blank or use an asterisk (*) to replace it.
- **account-id**: the ID of the account. The value **system** indicates public system resources, such as system-defined identity policies.
- **type-name**: the resource type that supported by the target cloud service. For details, see the resource type description of each service in **Identity Policy–based Authorization**.
- **resource-path**: the resource path. For details, see the resource type description of each service in **Identity Policy–based Authorization**.

# 3 Functions

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

**NOTICE**

IAM ensures eventual consistency for its functionalities. Operations performed within IAM, such as creating users and user groups or granting authorizations to these entities, might experience delayed effects due to data replication across various servers in data centers of Huawei Cloud, facilitating multi-region data sync. It is advisable to verify that any committed policy changes have been effectively implemented prior to proceeding with further actions.

## Refined Permissions Management

You can grant IAM users permissions to manage different resources in your account.

## Secure Access

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.

## 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.

## Policy Attachment to Users

You can directly attach policies to users for agile, flexible permissions control.

## 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 verification and password policies improve security of user information and system data.

## Access Analyzer

IAM Access Analyzer helps identify resources and unused passwords and keys (such as OBS bucket policies, KMS keys, IAM agencies, or trust agencies) that are shared with external principals in your organization or account.

IAM Access Analyzer can:

- Identify resources in your account or organization that are shared with an external principal.

  IAM Access Analyzer analyzes your resources to identify unintended external access to your resources.
- Identify unused access in your organization or account.

  Unused access analyzers generate findings for unused access. The findings provide visibility into unused passwords, access keys and permissions, and unused permissions of trust agencies for IAM users in your organization or account.
- Validate custom policies against policy grammar.

  The access analyzer checks your policy against policy grammar and provides check findings. The check results include security warnings, errors, suggestions, and general warnings.

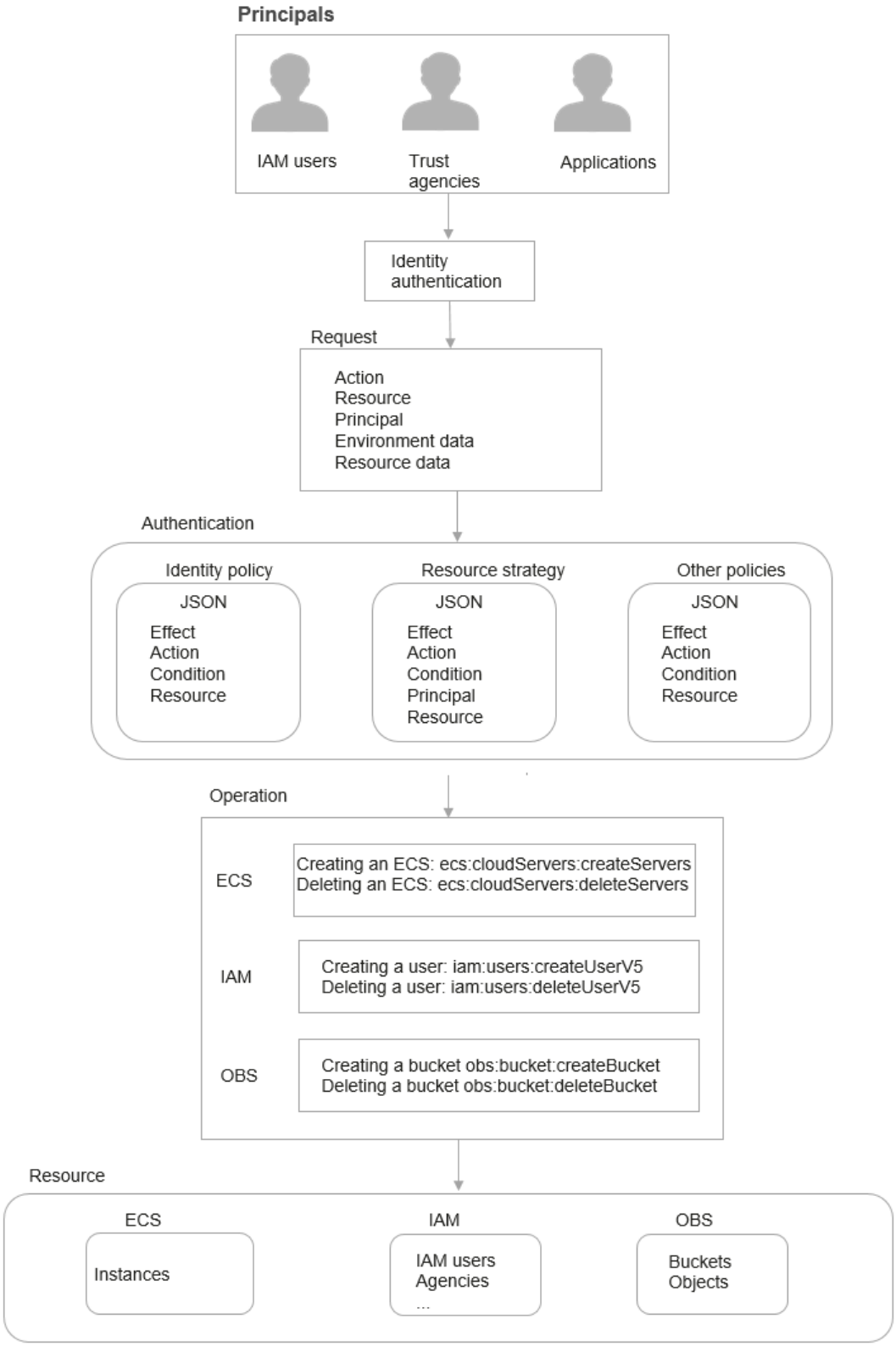
# 4 How IAM Works

IAM provides the infrastructure for authentication and authorization of your account.

When a user logs in to the console or uses an application to access an API, IAM matches the credentials to an IAM principal (such as an IAM user and trust agency) and authenticates their permissions to access Huawei Cloud. IAM allows or denies access in response to an authentication request. For example, when you first log in to Huawei Cloud and access the console home page, you are not accessing any cloud service. When you select a cloud service, you send an authorization request to IAM for that service. IAM verifies whether your identity is on the list of authorized users, evaluates any policies that may be in effect, and provides the final authentication result. Once authorized, you can perform operations in your account, such as creating ECS instances, creating IAM users, and deleting OBS buckets. The following figure shows the IAM authentication and authorization process:

**Figure 4-1** IAM authentication and authorization process



## Identity Authentication

When a principal logs in to Huawei Cloud using credentials, IAM authenticates the principal before allowing the principal to send a request to Huawei Cloud. Each type of users must be authenticated.

- Root user: Your credentials used for authentication are the HUAWEI ID/ Huawei Cloud account name and password you specified.
- IAM user: Your credentials used for authentication are your account name, IAM username, and password.
- Federated user: Your identity provider authenticates you and passes your credentials to Huawei Cloud. You do not need to log in to Huawei Cloud. Both IAM Identity Center (external identity source) and the old IAM console support identity federation.
- IAM Identity Center user (local identity source): Users created in IAM Identity Center log in via the IAM Identity Center user portal and provide your username and password.

You are advised to enable MFA for all users to enhance account security. For more information about MFA, see **Multi-Factor Authentication**.

## Components of a Request

When a principal tries to access the Huawei Cloud console, API, or CLI, the principal sends a request to Huawei Cloud. The request contains the following information:

- Action: the action that the principal wants to perform
- Resource: the Huawei Cloud resource upon which the principal requests to perform an operation
- Principal: the person (such as an IAM user, a trust agency, and an application) who sends the request
- Environment data: information about the IP address, time, and user agent in the request
- Resource data: data related to the requested resource, such as the tags of an IAM user and trust agency

Huawei Cloud collects request information into the **request context**. IAM evaluates the request context to authenticate the request.

## Authorization and Permission Policy Basics

Authentication determines whether a principal has the permissions required to complete its request. During authentication, IAM uses the value in the request context to determine whether to allow or deny the request. There are many types of policies that can affect a request authentication. You can use an IAM identity policy to grant your IAM users permissions to access Huawei Cloud resources in your account. You can use a resource-based policy to grant permissions across accounts. For cross-account access, the resource-based policy in another account must allow you to access its resources, and the IAM principal that you use to make the request must be allowed by the identity policy.

IAM checks each policy applied to the request context. IAM evaluation uses an **explicit deny**. If a policy includes a denied action, IAM denies the entire request

and stops the evaluation. If no authorization is performed, the request is denied by default. An applicable policy must allow every part of your request for IAM to authorize your request. The evaluation logic for a request within a single account follows these basic rules:

- By default, all requests are denied. (Generally, requests made using the account root user to access resources in the account are always allowed.)
- An explicit allow in any policy (identity-based or resource-based) overrides this default.
- The existence of a service control policy (SCP) or a session policy overrides the allow. If one or more of these policy types exists, they must all allow the request. Otherwise, it is implicitly denied. For more information about SCPs, see **SCP Introduction** in the *Organizations User Guide*.
- An explicit deny in any policy overrides any allows in any policy.

For more information, see **Request Context**.

After authentication, IAM determines whether to allow the request based on the policies attached to the IAM identity. Each Huawei Cloud service defines the actions they support and operations they can perform on resources, such as creating, viewing, editing, and deleting resources. For example, IAM defines dozens of actions for user resources, including the following basic actions:

- Action for creating a user: iam:users:createUserV5
- Action for viewing a user: iam:users:getUserV5
- Action for editing a user: iam:users:updateUserV5
- Action for deleting a user: iam:users:deleteUserV5

In addition, you can specify conditions in your policy to allow access to resources when the request meets the specified conditions. For example, you might want a policy statement to take effect after a specific date or to control access when a specific value appears in an API. For details, see **Global Condition Keys**.

After IAM allows a request, the principal can use resources in your account. Resources are objects in Huawei Cloud services, such as ECS instances, IAM users, and OBS buckets. If the principal creates a request to perform an action on a resource that is not included in the policy, the service denies the request. For example, if you have permission to create IAM users but request to create IAM user groups, the request fails if you do not have permission to create IAM user groups. For details about the supported actions, resources, and condition keys supported by different services, see **Identity Policy–based Authorization**.

# 5 Personal Data Protection

To prevent personal data (such as the username or password) from being accessed by unauthorized entities or individuals, IAM encrypts the data before storing it, controls access to the data, and can check all operations performed on the data from operation logs.

## Personal Data

Table 5-1 lists the personal data generated or collected by IAM.

**Table 5-1** Personal data

| Type | Source | Modifiable | Mandatory |
| --- | --- | --- | --- |
| Username. | • Entered when you create a user on the management console.<br>• Entered when you call an API. | No | Yes<br>Usernames are used to identify users. |
| Password | • Entered when you create a user or reset the password on the management console.<br>• Entered when you call an API. | Yes | No<br>You can also choose AK/SK authentication. |
| AK/SK | Created on the **My Credentials** page or the IAM console. | No<br>AK/SK cannot be modified, but they can be deleted and created again. | No<br>AK/SK are used to sign the requests sent to call APIs. |

## Personal Data Storage

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

- Usernames and AKs: non-sensitive data, which is stored in plaintext.
- Passwords and SKs: encrypted

## Access Control

Personal data is stored in the IAM database after being encrypted. A whitelist is configured to control access to the database.

## API Constraints

- AK/SK authentication is required for calling APIs. You can create an access key (AK/SK) and download the file containing the access key. If you are unable to locate the file, you can create an access key again and download the file. Do not share your access key with anyone else.
- IAM does not provide APIs for batch querying and modifying personal data.

## Operation Logs

IAM logs all personal data operations, including adding, modifying, querying, and deleting personal data. It uploads operation logs to CTS, and allows users to query only their own operation logs.

# 6 Differences Between the Old and New IAM Consoles

The new IAM console provides more refined and flexible permission control than the old console. Some functions are deleted to help you focus on IAM access control capabilities. The following details the differences between the old and new IAM consoles.

## Users

**Table 6-1** Differences of IAM users on the old and new IAM consoles

| Function | Item | Old Console | New Console |
| --- | --- | --- | --- |
| User creation | Batch creation | Supported | Not supported |
| | User details setting | Username, description, mobile number, email address, external identity ID, access type, credential type, and login protection | Username and description |
| | Creation method | Creating a user on the IAM console | Creating a user on the IAM Identity Center console (recommended) or on the IAM console |
| | Authorization | Inheriting permissions from user groups | Inheriting permissions from user groups or attaching identity policies to users |
| User management | Batch deletion | Supported | Supported |

| Function | Item | Old Console | New Console |
| --- | --- | --- | --- |
| | Batch modification | Supported (status, access type, authentication mode, login password, mobile number, and email address) | Supported (status and login password) |
| | User details export | Supported (exporting information about all users) | Supported (exporting information about selected or all users) |
| | Modification of user details | User status and description | Username, status, and description |
| | Tagging | Not supported | Supported |
| | Access Mode | Changing the access mode to restrict user access. | Enabling or disabling "Manage Console Access" to restrict console access, and determining whether to allow API calls via programmatic access by creating AK/SK for users |
| Security settings | Login credentials | Login password reset, password deletion, and last password change time | Console access disable (by deleting the password), password reset, and password update time, password expiration time, and last login time |
| | Multi-factor authentication (MFA) | Virtual MFA devices or security keys | Virtual MFA devices or security keys |
| | Login protection | Supported | Not supported |

## User Groups

The search capability is enhanced. You can filter user groups by user group name, description, and creation time.

## Policy

The new IAM console supports more condition keys for fine-grained permission control.

**Table 6-2** Differences of policies on the old and new consoles

| Item | Old Console | New Console |
| --- | --- | --- |
| Navigation pane | Authorization and Policies/ Roles | Identity policies |
| Authorization | Both IAM authorization and enterprise project authorization are supported. | Only IAM authorization is supported. You can use the condition key **g:EnterpriseProjectId** to control the authorization scope of enterprise projects. |
| Capability | Policies can be attached on the **User Groups** and **Agencies** pages only. After the enterprise project function is enabled, you can use policies to directly authorize users for specific enterprise projects. | You can attach identity policies to or detach identity policies from IAM identities (users, user groups, agencies, and trust agencies). |
| Authorization object | System-defined policies, system-defined roles, and custom policies can be attached only to user groups and agencies. After the enterprise project function is enabled, you can attach system-defined policies and custom policies to users for specific enterprise projects. | System-defined policies and custom identity policies can be attached to users, user groups, agencies, and trust agencies. |

The following policy denies access to Huawei Cloud service platforms based on the source IP address:

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "*:*:*"
        ],
        "Condition": {
            "NotIpAddress": {
                "g:SourceIp": [
                    "192.0.2.0/24",
                    "10.27.128.0/24"
                ]
            }
        }
    }]
}
```

The following policy allows only IAM users whose names start with **TestUser** to query enterprise route instance details:

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["er:instances:get"],
         "Resource": ["*"],
         "Condition": {
            "StringMatch": {
               "g:UserName": [
                  "TestUser*"
               ]
            }
         }
      }
   ]
}
```

## Project

The new IAM console does not support projects. You can use condition key **g:ProjectId** to control the authorization scope of projects (see the following policy). If you still want to use project-based authorization, go to the old IAM console.

The following example policy only allows VPCs to be created in the IAM project identified by **10a6c23c2a1044779794798beb067c94**:

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["vpc:vpcs:create"],
         "Resource": ["*"],
         "Condition": {
            "StringEquals": {
               "g:ProjectId": "10a6c23c2a1044779794798beb067c94"
            }
         }
      }
   ]
}
```

The following example policy only allows queries to ECS details in the IAM project **10a6c23c2a1044779794798beb067c94**:

```
{
   "Version": "5.0",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": ["ecs:cloudServers:showServer"],
         "Resource": ["*"],
         "Condition": {
            "StringEquals": {
               "g:ProjectId": "10a6c23c2a1044779794798beb067c94"
            }
         }
      }
   ]
}
```

## Agency

**Table 6-3** Differences of agencies on the old and new consoles

| Function | Item | Old Console | New Console |
| --- | --- | --- | --- |
| Agency list | Viewing the agency list | You can only view agencies created on the old console. | You can view agencies created on the old console and trust agencies created on the new console. |
| Agency creation | Creating an agency | You cannot set trust policies for agencies created. | You can set trust policies for trust agencies created. |
| | Creating an account agency | You can specify the account name. | You can specify the account ID. |
| | Expression of delegation duration | Validity period | Maximum session duration |
| | Option | None | External ID and MFA |
| | Edit mode | None | Trust policy |
| | Authorization scope setting | Assigning permissions and setting the scope | None (Authorization can be performed separately after the agency is created.) |
| Agency details | Display of details | Agency type and account name | URN only |
| | Authorization records | Displayed | None |

## Identity Providers

The new IAM console does not support identity providers. You can use **Identity Source** in IAM Identity Center. If you still want to use identity providers, go to the old IAM console.

## Security Settings

The new IAM console does not provide the following settings:

- Login password, mobile number, and email address
- Critical operation protection
- ACL, which is integrated into the login authentication policy setting. You are advised to use the "Condition" key in permission policies to restrict access by IP address range.

## My Credentials

Login credentials and MFA device functions are available on the new console. You can manage the password of an identity that has logged in to the console. You can check the password expiration time and the last time when the password was changed. You can bind and unbind MFA devices, including virtual MFA devices and security keys. If you are using a HUAWEI ID, you need to go to the account and security page to bind a virtual MFA device to your HUAWEI ID. It is used for identity authentication during login and operation protection.

# 7 IAM-based Permissions Management

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 and assign permissions to control their access to specific resources. For example, if you want project planners in your company to view IAM details but do not want them to delete IAM users or perform any other high-risk operations, you can create IAM users and grant permission to view IAM but not permission to delete. For the system-defined permissions supported by IAM, see **System-defined Identity Policies**.

## IAM Permissions

**Table 7-1** lists all the system-defined identity policies for IAM.

**Table 7-1** System-defined identity policies

| Name | Description | Type |
| --- | --- | --- |
| IAMFullAccessPolicy | Full permissions for IAM. | System-defined identity policy |
| IAMReadOnlyPolicy | Read-only permissions for IAM. | System-defined identity policy |

**Table 7-2** lists the common operations supported by system-defined identity policies for IAM.

**Table 7-2** Common operations supported by system-defined permissions

| Operation | IAMFullAccessPolicy | IAMReadOnlyPolicy |
| --- | --- | --- |
| Creating IAM users | Yes | No |
| Querying IAM user details | Yes | Yes |
| Modifying IAM user information | Yes | No |
| Querying security settings of IAM users | Yes | Yes |
| Modifying security settings of IAM users | Yes | No |
| Deleting IAM users | Yes | No |
| Creating user groups | Yes | No |
| Querying user group details | Yes | Yes |
| Modifying user group information | Yes | No |
| Adding users to user groups | Yes | No |
| Removing users from user groups | Yes | No |
| Deleting user groups | Yes | No |
| Assigning permissions to user groups | Yes | No |
| Removing permissions of user groups | Yes | No |
| Creating custom identity policies | Yes | No |
| Modifying custom identity policies | Yes | No |
| Deleting custom identity policies | Yes | No |
| Querying permission details | Yes | Yes |
| Creating trust agencies | Yes | No |

| Operation | IAMFullAccessPolicy | IAMReadOnlyPolicy |
| --- | --- | --- |
| Querying trust agencies | Yes | Yes |
| Modifying trust agencies | Yes | No |
| Switching roles | Yes | No |
| Deleting trust agencies | Yes | No |
| Granting permissions to trust agencies | Yes | No |
| Removing permissions of trust agencies | Yes | No |
| Querying quotas | Yes | Yes |

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 FullAccess permission.

**Table 7-3** Access key operations supported by system-defined permissions

| Operation | IAMFullAccessPolicy | IAMReadOnlyPolicy |
| --- | --- | --- |
| Creating access keys (for other IAM users) | Yes | No |
| Querying access keys (of other IAM users) | Yes | Yes |
| Modifying access keys (for other IAM users) | Yes | No |
| Deleting access keys (for other IAM users) | Yes | No |

## Content of IAMFullAccessPolicy

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:*:*"
      ]
    }
```

```
  ]
}
```

## Content of IAMReadOnlyPolicy

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:*:get*",
        "iam:*:list*",
        "iam:*:check*",
        "iam:*:show*"
      ]
    }
  ]
}
```

# 8 Permissions Management Based on ABAC

In IAM, authorization is the key to ensuring that principals have the correct access permissions. There are two types of models to implement access control: attribute-based access control (ABAC) and role-based access control (RBAC). Understanding the differences between the two models helps you design more secure and efficient access control solutions.

## Definition

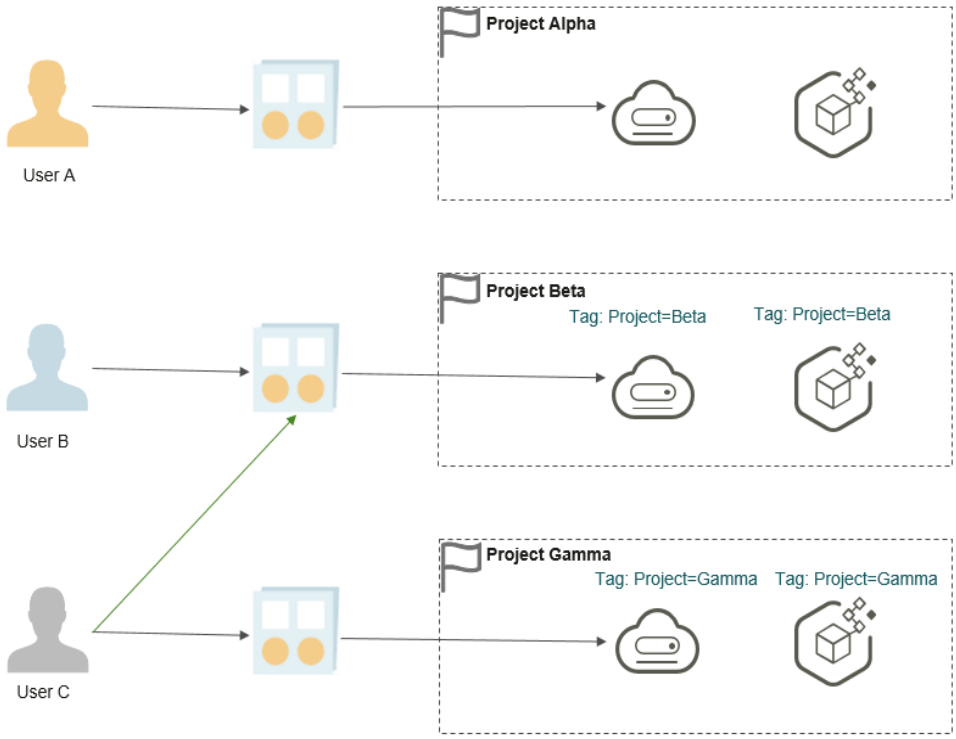
- **ABAC**: ABAC is an authorization strategy that is attached to IAM identities (such as IAM users) and defines permissions based on attributes. It uses policies to determine access authorization in real time based on a combination of attributes such as subjects, resources, operations, and environments. For example, you can specify that only users with the **Project=Alpha** tag can access resources with the **Project=Alpha** tag.
- **RBAC**: RBAC is a strategy that defines permissions based on a user's function or role in an organization. In IAM, you implement RBAC by creating different policies or using predefined roles on Huawei Cloud for different job functions. You then attach the policies to IAM identities (such as IAM users) and restrict their access (such as within a project). For example, you can assign the Huawei Cloud predefined CCE Administrator role to a container administrator and restrict its permissions to project **Alpha**.

In the following example, employees need to work on three projects (**Alpha**, **Beta**, and **Gamma**) and access ECS resources, you can assign the ECS Administrator role to them and restrict their permissions to these projects respectively. Then, they can access cloud service resources only within the authorized scope. If an employee's job changes and the employee needs to access the containers provided by CCI, or user C needs to access resources in project **Beta**, you must create a new role authorization relationship and update the authorization scope.

With ABAC, you can create identity policies to allow specific identities to access cloud service resources with specific tags (for example, **Project=Beta** or **Project=Gamma**). You can manage access control for identities or resources based on tags, without repeatedly adjusting policies or authorization relationships.

**Figure 8-1** An example




## Core Differences

**Table 8-1** Core differences

| Feature | RBAC | ABAC |
| --- | --- | --- |
| **Authorization relationship** | Identities - Roles - Permission Scope | Identities - Policies |
| **Authorization basis** | Predefined roles and functions | Dynamic attributes of identities, resources, environments, etc. |
| **Number of policies** | More policies are often needed as functions and resources increase. | Fewer policies are usually required because policies are based on attributes rather than a specific principal. |
| **Scalability** | You may need to update existing policies manually when adding new resources or functions. | Permissions can be automatically extended with new resources. You do not need to modify existing policies. |
| **Permission granularity** | Access permissions to specific resources are usually granted. | Access is authorized based on diverse condition control attributes. |

| Feature | RBAC | ABAC |
| --- | --- | --- |
| **Management complexity** | It may become complex in large or rapidly changing environments. | It is easier to manage permissions of new projects or personnel changes. |

NOTE

1. IAM policies implement policy-based roles. The authorization is based on the identity-role-authorization scope relationship. Identity policies, however, are based on the identity-policy relationship.
2. IAM identity policies support complete ABAC access control conditions, including dynamic attributes based on identities, resources, and environments. Compared with policies, identity policies support more access control condition keys. For details, see **Global Condition Key**. In addition, identity policies support richer policy syntax. For details, see **JSON Element Reference**.

## Advantages of ABAC over RBAC

- **Dynamic response to changes and growth**: Permissions for new resources are automatically granted as long as the attributes match. You do not need to manually assign policies to identities. This greatly simplifies permissions management when new projects start or team members change.
- **More fine-grained access control**: ABAC allows you to use attributes based on principals, resources, actions, and environment contexts.
- **Fewer policies and easier management**: ABAC usually requires fewer policies. You do not need to create separate policies for each job function, so you can easily manage and maintain policies.
- **Integration with enterprise identity providers**: ABAC allows you to map employee attributes on an external identity provider (IdP) to IAM identity tags (via IAM Identity Center) and control access based on these tags. For details, see **ABAC Overview and Configuration Process**.

# 9 Security

## 9.1 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.

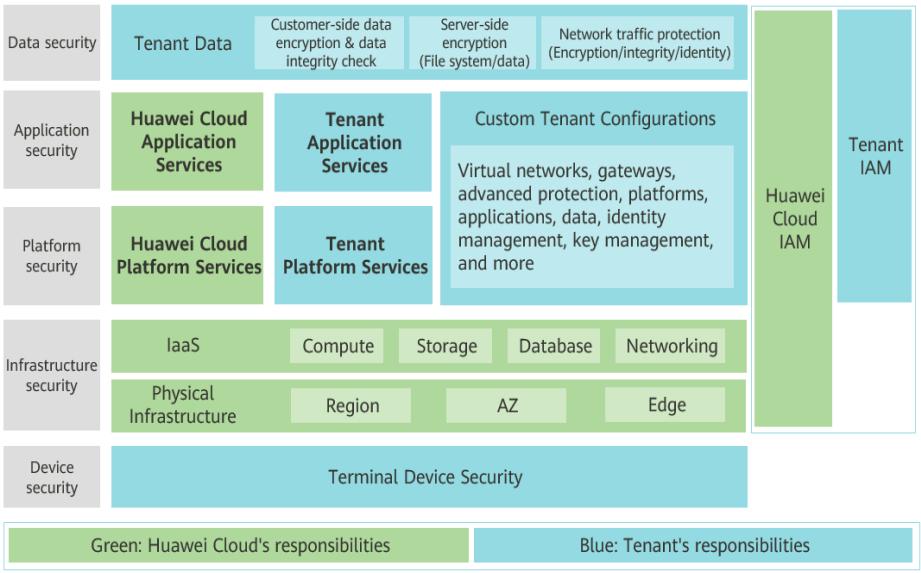
**Figure 9-1** illustrates the responsibilities shared by Huawei Cloud and IAM users.

- **Huawei Cloud responsibility "Security of the Cloud"**: Huawei Cloud is responsible for protecting the Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) that offered in the Huawei Cloud and the physical environments of the Huawei Cloud data centers that run these services. Huawei Cloud is responsible not only for the security functions and performance of the infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and security compliance.
- **Tenant responsibility "Security in the Cloud"**: 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 9-1** Huawei Cloud shared security responsibility model




# 9.2 Authentication and Access Control

## 9.2.1 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 and passwords, access keys, and temporary security credentials. IAM implements security design for each identity credential to protect user data and enable users to access IAM more securely. For details, see **Table 9-1**.

**Table 9-1** IAM identity credentials and security design

| Access Credential | Principal | Security Description | Reference |
| --- | --- | --- | --- |
| Username and password | Account root users and IAM users | You can configure the character type and minimum length of a user password as required. You can also configure the password validity period policy and minimum password validity period policy. | **Password Policy** |

| Access Credential | Principal | Security Description | Reference |
| --- | --- | --- | --- |
| Access Key | Account root users and IAM users | AK is used together with SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct. | Access Keys |
| Temporary security credential | Agency or trust agency | 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 Security Credentials |

## Login Protection and Verification Policy

As described in Table 9-2, 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 9-2** Login authentication policy

| 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).<br>Verify that virtual MFA devices are supported. For details, see **Multi-Factor Authentication**. | Login Protection |

| Login Protection Method | Description | Functions |
| --- | --- | --- |
| Login Authentication Policy | IAM supports the **session timeout** policy. If a user does not log in to the system within a specified period, the user needs to log in again. IAM supports the **account lockout** policy. If the number of login failures exceeds the threshold, the account is locked. IAM supports the **account disabling** policy. If a user does not log in to the system for a long time, the account is disabled. IAM supports the display of **recent login information** to allow users to view the last login time. | **Login Authentication Policy** |

## 9.2.2 Access Control

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

**Table 9-3** IAM access control

| Access Policy | Description | Reference |
| --- | --- | --- |
| IAM Fine-grained Authorization Policy | IAM service permissions are divided into fine-grained policies. Identity policies define the user operations allowed or rejected by IAM. For example, if a user or user group has the IAM ReadOnlyAccessPolicy permissions, the user or user group only has the read-only permissions for IAM service data. IAM also supports **custom identity policies** to assign IAM service permissions. | **IAM Permissions** |

| Access Policy | Description | Reference |
| --- | --- | --- |
| ACL | With ACL, you can set access control policies to allow users to log in to the IAM console only from specified IP address ranges and network segments. | Login authentication policy |

# 9.3 Data Protection

## 9.3.1 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 principals or individuals, IAM encrypts your data during storage and transmission to prevent data leakage.

### Personal Data

Table 9-4 lists the personal data generated or collected by IAM.

**Table 9-4** Personal data

| Type | Source | Description | Modifiable | Mandatory |
| --- | --- | --- | --- | --- |
| Username | • Entered when you create an IAM user or modify a username.<br>• Entered when you call an API. | • User identity identification<br>• Identity authentication during console access or API calling | Yes (Administrators can change the username via the console or API.) | Yes<br>Usernames are used to identify users. |
| Password | Entered when you create a user or reset the password on the console. | Identity authentication during console access | Yes | No<br>You can also choose AK/SK authentication. |

| Type | Source | Description | 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<br>AK/SK cannot be modified, but they can be deleted and created again. | No<br>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, stored in plaintext.
- Passwords: encrypted by the salted SHA512 or SM3 and then stored.
- SKs: encrypted by AES or SM4 and then stored.

### 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.

## 9.3.2 User 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. Users 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 **Security Best Practices in IAM**.

# 9.4 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.

# 9.5 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 **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 **Enabling CTS**. After CTS is enabled, you can **view IAM audit logs**. CTS stores operation logs of the last seven days.

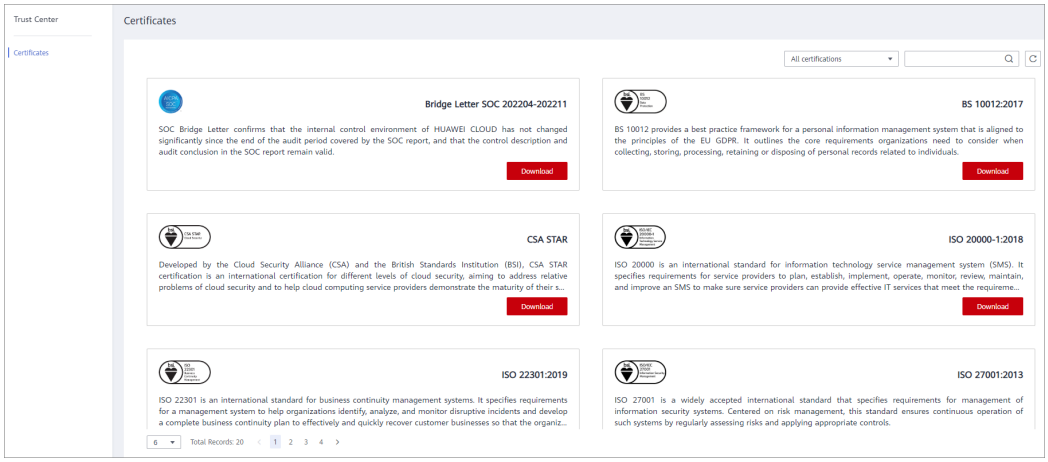
CTS allows you to **configure key event notifications**. You can add IAM-related high-risk and sensitive operations as key operations to the real-time monitoring list of CTS for monitoring and tracing. If a key operation in the monitoring list is triggered when a user uses the IAM service, CTS records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

# 9.6 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 9-2** Downloading compliance certificates

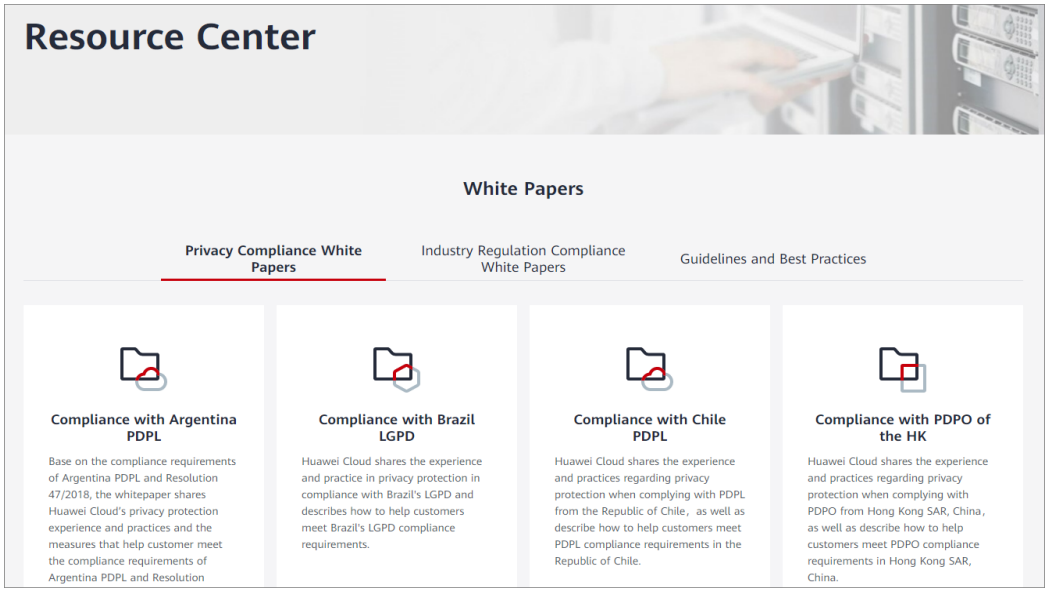



## Resource Center

Huawei Cloud also provides the following resources to help you meet compliance requirements. For details, see **Resource Center**.

**Figure 9-3** Resource center



# 10 Notes and Constraints

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

| Category | Item | Default Quota | Maximum Value | Adjustable |
|---|---|---|---|---|
| User | IAM users | 50 | 2000 | Yes |
| | Characters allowed in a username | 64 | - | No |
| | Identity policies you can attach to a user | 10 | 20 | √ |
| | User groups a user can belong to | 10 | - | No |
| | AK/SK pairs that a user can create | 2 | - | No |
| | Virtual MFA devices you can add to a user | 1 | - | No |
| User group | User groups | 20 | 2000 | Yes |
| | Characters allowed in a user group name | 128 | - | No |
| | Users you can add to a user group | IAM users in your account | - | No |
| | Identity policies you can attach to a user group | 10 | - | No |
| Agency and trust agency | Characters allowed in a trust agency name | 64 | - | No |
| | Total agencies and trust agencies | 50 | 5000 | Yes |

| Category | Item | | Default Quota | Maximum Value | Adjustable |
|---|---|---|---|---|---|
| | Permissions (including system-defined and custom identity policies) assigned to an agency or trust agency | | 10 | 20 | Yes |
| Identity policy | Custom identity policies | | 1,500 | 5000 | Yes |
| | Custom identity policy versions | | 5 | - | No |
| | Characters allowed in an identity policy name | | 128 | - | No |
| | Custom identity policy | Bytes | 6,144 | - | No |
| | | Bytes allowed in a statement | There is no limit for each statement, but the total number of bytes of an identity policy cannot exceed 6,144. | - | No |
| | | Bytes allowed in an action | There is no limit for each action, but the total number of bytes of an identity policy cannot exceed 6,144. | - | No |

| Category | Item | | Default Quota | Maximum Value | Adjustable |
|---|---|---|---|---|---|
| | | Bytes allowed in a resource | There is no limit for each resource, but the total number of bytes of an identity policy cannot exceed 6,144. | - | No |
| | | Bytes allowed in a condition | There is no limit for each condition, but the total number of bytes of an identity policy cannot exceed 6,144. | - | No |