Identity and Access Management

Best Practices

Issue   02
Date   2024-12-25

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Recommendations for Using IAM

To establish secure access to your Huawei Cloud resources, follow these recommendations for the Identity and Access Management (IAM) service.

Do Not Create Access Keys for Your Account

Your account has all the permissions required to access resources and make payments for the usage of resources. Both passwords and access keys (AKs/SKs) are account credentials, and they have the same effect. Passwords are mandatory and used for console login. Access keys are optional, supplementary to passwords, and used for programmatic requests with development tools. Access keys can be lost or accidentally disclosed. To enhance account security, do not create access keys for your account.

Do Not Write Access Keys into Code

If you use APIs, CLI tools, or SDKs to access cloud services, do not write your access keys into the code.

Create Individual IAM Users

If someone needs to access resources in your account, do not share your password with them. Instead, create an individual IAM user for them and grant required permissions to the IAM user. You can also create an IAM user for yourself, grant the IAM user administrator permissions, and perform routine management using the IAM user.

Set Appropriate Access Type

You can set the access type of IAM users, including programmatic access and management console access. Note the following when you set the access type:

- If the user accesses Huawei Cloud services only by using the management console, select **Management console access** for **Access Type** and **Password** for **Credential Type**.
- If the user accesses Huawei Cloud services only through programmatic calls, select **Programmatic access** for **Access Type** and **Access key** for **Credential Type**.

- If the user needs to use a password as the credential for programmatic access to certain APIs, select **Programmatic access** for **Access Type** and **Password** for **Credential Type**.
- If the user needs to perform access key verification when using certain services in the console, such as creating a data migration job in the Cloud Data Migration (CDM) console, select **Programmatic access** and **Management console access** for **Access Type** and **Access key** and **Password** for **Credential Type**.

Grant Least Privilege

It is a standard security measure to grant users only the permissions required to perform specific tasks. You can achieve this by using IAM's system-defined or custom policies. The principle of least privilege (PoLP) helps you establish secure access to your Huawei Cloud resources.

For IAM users who access cloud services by using APIs, CLI tools, or SDKs, grant them permissions by using custom policies to minimize impact due to accidental access key disclosure or loss.

Enable Virtual MFA

Multi-factor authentication (MFA) adds an additional layer of security protection on top of the identity credentials for an account. It is recommended that you enable MFA authentication for your account and privileged users created using your account. To log in to the management console, users must enter their usernames and passwords and a verification code generated by the bound virtual MFA device.

An MFA device can be based on hardware or software. Currently, Huawei Cloud supports software-based virtual MFA devices. It is a program that runs on a portable device (such as a mobile phone) and generates a six-digit verification code for identity authentication.

Set a Strong Password Policy

To ensure that IAM users only use complex passwords and change them periodically, set a password policy to define strong password requirements, such as minimum password length, and whether to allow consecutive identical characters in a password, and whether to allow previously used passwords.

Enable Critical Operation Protection

Enable critical operation protection to prevent misoperations. When you or users created using your account perform critical operations, such as deleting resources or generating access keys, you and users need to provide verification codes to proceed with the operations.

Periodically Change Your Identity Credentials

Periodically changing your password and access keys can prevent risks caused by their accidental disclosure or loss.

- Set a password validity period to require you and users created using your account to change passwords. IAM will start to display a prompt 15 days before a password expires.
- You can create two access keys and use them interchangeably. For example, you can use access key 1 for a certain period, and then use access key 2 for the next period. You can also delete access key 1 and generate another access key.

Delete Unnecessary Identity Credentials

For users who only need to use the console, it is recommended that you do not create access keys for them, and delete any access keys that have already been created. If a user has not logged in for a long period, change the user's password and delete the user's access keys. In addition, set an account validity period to automatically disable user accounts that have not been used for a long time.

Delegate Resource Access to Applications Running on ECSs

Applications running on Elastic Cloud Servers (ECSs) can access other Huawei Cloud services only with a credential provided. To securely provide credentials for applications, create an agency in IAM to grant required permissions to the ECS where the applications run, and configure the agency for the ECS so that the applications can obtain temporary access keys. The ECS applies for a temporary credential from IAM to securely access resources based on the permissions granted through the agency. ECS automatically rotates temporary credentials to ensure that they are secure and valid.

When you start an ECS, you can specify an agency for the ECS as a startup parameter. Applications running on the ECS can access Huawei Cloud resources by providing the temporary access key obtained using the agency. The agency determines which applications can access specific resources.

Enabling CTS

Cloud Trace Service (CTS) is a log audit service provided by Huawei Cloud. It collects, stores, and queries records of operations on IAM, facilitating security analysis, compliance audit, resource tracking, and fault locating. It is recommended that you enable the CTS service to record key IAM operations, such as creating and deleting IAM users.

2 Assigning Permissions to O&M Personnel

Assume that a company has purchased different resources on Huawei Cloud, and has multiple functional teams that need to use one or more types of resources. The company can use IAM to assign permissions to different personnel based on their job functions for refined permissions control.

Figure 2-1 Permissions management model
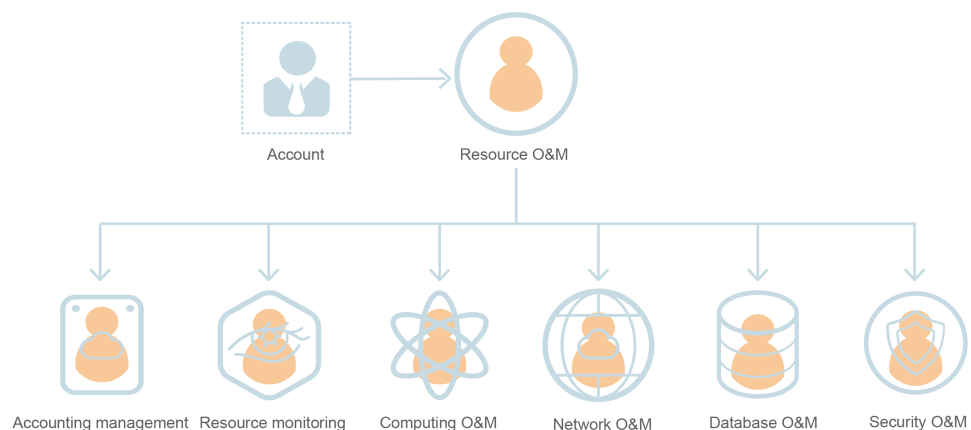
- Resource O&M team

- Accounting management team

- Resource monitoring team

- Computing O&M team

- Network O&M team

- Database O&M team

- Security O&M team

Assign required permissions to different functional teams in the company according to **Table 2-1**. For details about permissions of all Huawei Cloud services, see **System-defined Permissions**.

Table 2-1 System-defined permissions

Functional Team	Policy	Permissions Description
Resource O&M team	Tenant Administrator	Full permissions for all cloud services, including Billing Center, Resource Center, and My Account, but excluding IAM. **Tenant Administrator** grants permission to purchase resources, manage renewals, and view bills.
Accounting management team	BSS Administrator	Full permissions for Billing Center, Resource Center, and My Account. The **BSS Administrator** role includes the permissions for managing invoices, orders, contracts, and renewals, and viewing bills. **Users assigned only this role cannot purchase resources unless you grant them the administrator permissions of the corresponding service.**
Resource monitoring team	Tenant Guest	Read-only permissions for all cloud services except IAM.
Computing O&M team	ECS FullAccess	Full permissions for Elastic Cloud Server (ECS), including permissions for purchasing ECS resources. Users assigned only the **ECS FullAccess** policy cannot view the usage of ECS resources and other resources unless you assign them the **BSS Administrator** role.

Functional Team	Policy	Permissions Description
	CCE FullAccess	Full permissions for Cloud Container Engine (CCE), including permissions for purchasing CCE resources. Users assigned only the **CCE FullAccess** policy cannot view the usage of CCE resources and other resources unless you assign them the **BSS Administrator** role.
	AutoScaling FullAccess	Full permissions for Auto Scaling (AS), including purchasing AS resources. Users assigned only the **AutoScaling FullAccess** policy cannot view the usage of AS resources and other resources unless you assign them the **BSS Administrator** role.
Network O&M team	VPC FullAccess	Full permissions for Virtual Private Cloud (VPC), including purchasing VPC resources. Users assigned only the **VPC FullAccess** policy cannot view the usage of VPC resources and other resources unless you assign them the **BSS Administrator** role.
	ELB FullAccess	Full permissions for Elastic Load Balance (ELB), including purchasing load balancers. Users assigned only the **ELB FullAccess** policy cannot view the usage of ELB resources and other resources unless you assign them the **BSS Administrator** role.

| Functional Team	Policy	Permissions Description
Database O&M team	RDS FullAccess	Full permissions for Relational Database Service (RDS), including purchasing RDS resources. Users assigned only the **RDS FullAccess** policy cannot view the usage of RDS resources and other resources unless you assign them the **BSS Administrator** role.
	DDS FullAccess	Full permissions for Document Database Service (DDS), including purchasing DDS resources. Users assigned only the **DDS FullAccess** policy cannot view the usage of DDS resources and other resources unless you assign them the **BSS Administrator** role.
	DDM FullAccess	Full permissions for Distributed Database Middleware (DDM).
Security O&M team	Anti-DDoS Administrator	Full permissions for Anti-DDoS.
	CAD Administrator	Full permissions for Advanced Anti-DDoS (AAD).
	KMS Administrator	Full permissions for Data Encryption Workshop (DEW), including purchasing DEW resources. Users assigned only the **KMS Administrator** role cannot view the usage of DEW resources and other resources unless you assign them the **BSS Administrator** role.

Assigning Permissions to O&M Personnel

The following is an example procedure for specifying an employee in the company as the network O&M owner in the **CN-Hong Kong** region. If you want to specify an employee as any other O&M owner, grant the required permissions to the employee according to **Table 2-1**.

### Step 1: Create a User Group and Assign Permissions

Step 1 Log in to the Huawei Cloud management console.

Step 2 On the management console, hover the mouse pointer over the username in the upper right corner and then choose **Identity and Access Management**.

Step 3 On the IAM console, choose **User Groups** in the navigation pane. Then click **Create User Group**.

Figure 2-2 Creating a user group
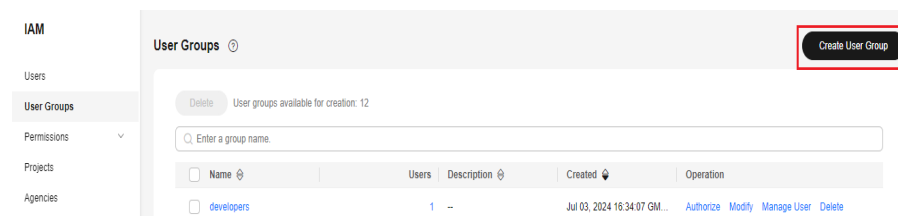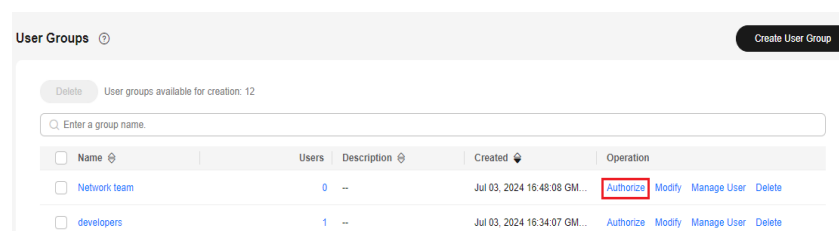

Step 4 Enter the user group name **Network_OM**, and click **OK**.

Figure 2-3 Entering a group name
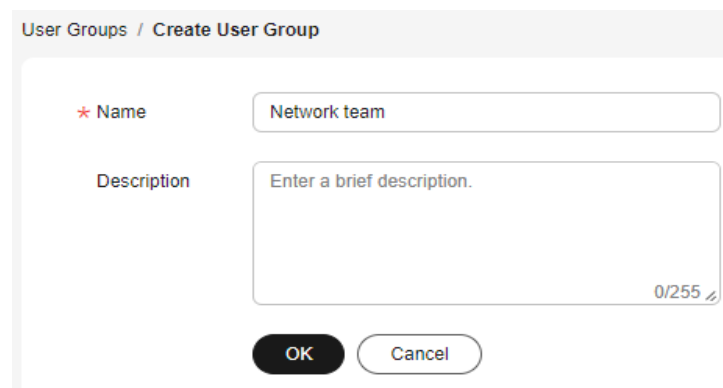
Step 5 In the row containing the user group, click **Authorize**.

Figure 2-4 Authorizing a user group

Step 6 Search for and select **VPC FullAccess** and **ELB FullAccess**, and click **Next**.

Step 7 Specify the authorization scope as **Region-specific projects** and select **CN-Hong Kong**.

☐ NOTE

- If users in the group need to view resource usage, attach the **BSS Administrator** role to the group for the same project.
- When specifying an employee as the security O&M owner according to **Table 2-1**, you must grant the employee other related permissions because the security services interwork with other cloud services. For more information, see **Assigning Dependency Roles**.

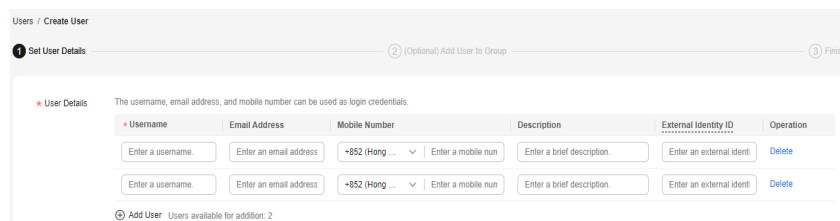**----End**

Step 2: Create an IAM User

Step 1 In the navigation pane of the IAM console, choose **Users**. Then click **Create User**.

Step 2 Specify the user details and access type. To create more users, click **Add User**. A maximum of 10 users can be created at a time.

Figure 2-5 Configuring user information

☐ NOTE

- Users can log in to Huawei Cloud using the username, email address, or mobile number.
- If users forget their password, they can reset it through email address or mobile number verification. If no email addresses or mobile numbers have been bound to users, users need to contact the administrator to reset their passwords.

Table 2-2 User information

Parameter	Description
Username	Username that will be used to log in to Huawei Cloud, for example, **James** and **Alice**. This field is required.
Email Address	Email address of the IAM user that can be used as a login credential. IAM users can bind an email address after they are created. This field is required if you have specified **Set by user** as the credential type.
Mobile Number	Mobile phone number of the IAM user that can be used as a login credential. IAM users can bind a mobile number after they are created. This field is optional.
Description	Additional information about the IAM user. This field is optional.

Figure 2-6 Setting the access type

- **Programmatic access**: Select this option to allow the user to access Huawei Cloud services using development tools, such as APIs, CLI, and SDKs. You can generate an **access key** or set a **password** for the user.

- **Management console access**: Select this option to allow the user to access Huawei Cloud services using the management console. You can set or generate a password for the user or request the user to set a password at first login.

    📖 **NOTE**

    – If the user **accesses cloud services only by using the management console**, select **Management console access** for **Access Type** and **Password** for **Credential Type**.

    – If the user **accesses cloud services only through programmatic calls**, select **Programmatic access** for **Access Type** and **Access key** for **Credential Type**.

    – If the user **needs to use a password as the credential for programmatic access** to certain APIs, select **Programmatic access** for **Access Type** and **Password** for **Credential Type**.

    – If the user needs to **perform access key verification** when using certain services in the console, select **Programmatic access** and **Management console access** for **Access Type** and **Access key** and **Password** for **Credential Type**. For example, the user needs to perform access key verification when creating a data migration job in the Cloud Data Migration (CDM) console.

Table 2-3 Setting the credential type and login protection

Credential Type and Login Protection		Description
Access key		After users are created, you can download the **access keys (AK/SK)** generated for these users. **Each user can have a maximum of two access keys.**
Password	Set now	Set a password for the user and determine whether to require the user to reset the password at first login. If you are the user, select this option and set a password for login. You do not need to select **Require password reset at first login**.
	Automatically generated	The system automatically generates a login password for the user. After the user is created, download the EXCEL password file and provide the password to the user. The user can then use this password for login. **This option is available only when you create a single user.**
	Set by user	A one-time login URL will be emailed to the user. The user can click on the link to log in to the console and set a password. If you do not use the IAM user, select this option and enter the email address and mobile number of the IAM user. The user can then set a password by clicking on the one-time login URL sent over email. The login URL is valid for **seven days**.
Login Protection	Enable (Recommended)	If login protection is enabled, the IAM user needs to enter a verification code in addition to the username and password during login. Enable this function for account security. You can select SMS, email, or virtual MFA device for verification during login.
	Disable	If login protection is disabled, you can enable it later by following the instructions provided in **Viewing or Modifying IAM User Information**.

Step 3 (Optional) Click **Next** to add the users to user groups.

- The user will inherit the permissions assigned to the user groups to which the user belongs.
- You can also create new groups as required.

📖 NOTE

- If the user will be an administrator, add the user to the default group **admin**.
- Each user can be added to multiple user groups.

Step 4 Click **Next**. If you have specified the access type as **Programmatic access** in **Step 2**, download the access key on the **Finish** page.

**Figure 2-7** Users created successfully
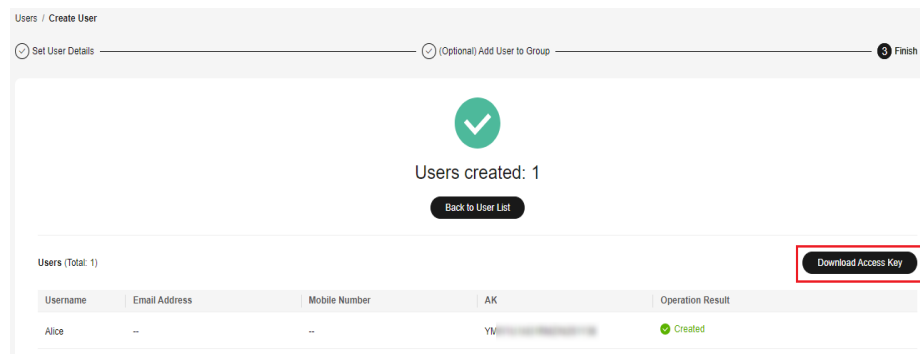
----End

Step 3: Log In as an IAM User and Verify Permissions

An IAM user can log in using different methods. The following describes how to log in through the login page. For more login methods, see **Logging In to Huawei Cloud**.

Step 1 On the Huawei Cloud login page, click **IAM User**.

Step 2 On the **IAM User Login** page, enter the account name, user name, and password of the created user.

Figure 2-8 Logging in as an IAM user
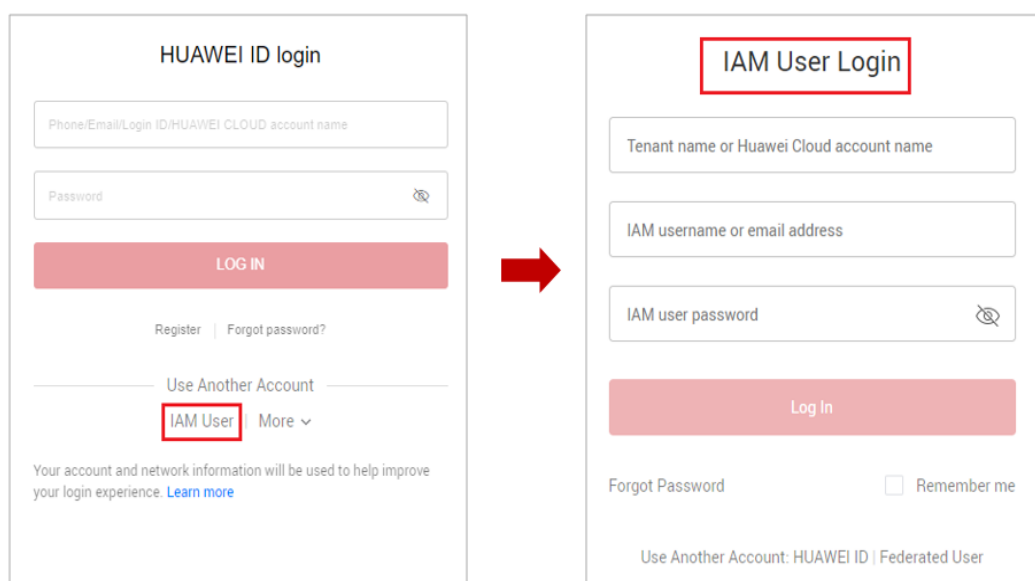
- Account name: Name of the account used to create the IAM user
- Username and password: The username and password specified for the IAM user

Step 3 On the management console, switch to the **CN-Hong Kong** region.

Step 4 Choose **Service List** > **Virtual Private Cloud**, **Elastic Load Balance**, and **Domain Name Service**, and perform operations on each service console to verify that the permissions have been successfully assigned.

Step 5 Choose a service other than the preceding services from **Service List** to ensure that the service cannot be accessed.

Step 6 On the management console, switch to a region other than **CN-Hong Kong** and ensure that the VPC, ELB, and DNS consoles cannot be accessed.

----End

3 Assigning System-defined Permissions for Common Cloud Services

Assign permissions for common cloud services to IAM users by referring to the following links:

- **Creating a User and Granting ECS Permissions**
- **Creating a User and Granting Permissions**
- **Creating a User and Granting Permissions**
- **Creating a User and Granting EVS Permissions**
- **Creating a User and Granting Permissions**
- **Cluster Permissions (IAM-based)**
- **Access Management on Department Public Data**
- **Creating a User and Granting CBR Permissions**
- **Creating a User and Granting VPC Permissions**
- **Creating a User and Granting DCS Permissions**
- **Creating a User and Granting Permissions**
- **Creating a User and Assigning Permissions**

# 4 Cross-Account Access Delegation and Resource Management

Company A and company B have created account A and account B, respectively. If account A wants to authorize account B to manage its resources, account A can create an agency in IAM to establish a trust relationship between the two accounts.

Requirements

- Account A has purchased different types of resources on Huawei Cloud. Account A wants to authorize account B to manage its VPC resources in the **CN-Hong Kong** region.

- Account B can authorize one or more employees (IAM users) of company B to manage account A's resources.

- Account A can modify or cancel the authorization provided to account B at any time.

Solution

- Account A creates an agency on the IAM console to authorize account B to manage its resources.

- Account B assigns permissions to its IAM users to manage account A's resources specified in the agency.

- Account A can modify or delete the agency at any time. Deleting the agency will automatically cancel the permissions assigned to account B and its IAM users for managing account A's resources.

Figure 4-1 Cross-account authorization model
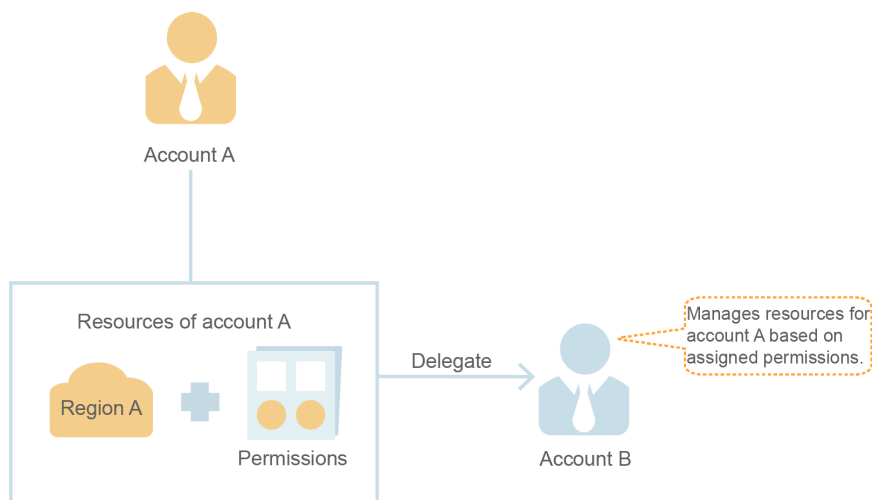
Delegating an Account to Manage Resources

Account A performs the following procedure to delegate account B to manage its VPC resources in the **CN-Hong Kong** region.

Step 1 Log in to Huawei Cloud using account A. On the IAM console, choose **Agencies** in the navigation pane.

Step 2 Click **Create Agency**, and enter an agency name, for example, **VPC Resources O&M**.

Step 3 Select the **Account** agency type, and enter the delegated account name, for example, **B-Company**.

Step 4 Set **Validity Period** to **Unlimited**.

Figure 4-2 Creating an agency

Step 5 Click **Done**.

Step 6 In the displayed dialog box, click **Authorize**.

Step 7 Select **VPC FullAccess** and click **Next**.

Step 8 Specify the authorization scope as **Region-specific projects**, and select **CN-Hong Kong**.

Step 9 Click **OK**.

The agency is displayed in the agency list.

📖 **NOTE**

Account A can modify the permissions or validity period of the agency or delete the agency based on service requirements.

----End

Managing Resources of an Account

After the agency is created, account B can switch roles to account A to manage account A's resources. To do this, account B needs to have obtained account A's account name and the agency name.

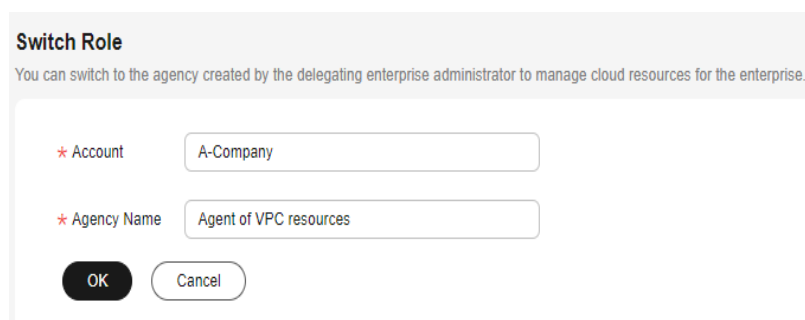**Step 1** Log in to the Huawei Cloud management console using account B.

Step 2 Click the username in the upper right corner, and choose **Switch Role**.

Figure 4-3 Switching roles
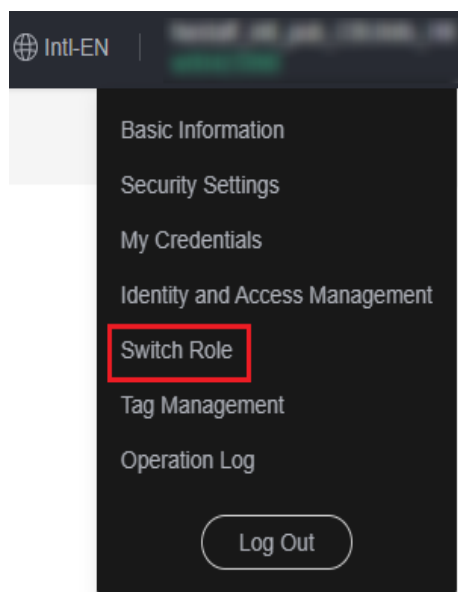
Step 3 Enter the account name of the delegating party. The agency created by the delegating party is displayed automatically.

Figure 4-4 Switching roles

Step 4 Click **OK** to switch to account A.

----End

5 Agency Configuration

5.1 Assigning Agency Permissions (by a Delegated Party)

Company B is a professional O&M company. It becomes a delegated party after being authorized by company A. Company B assigns permissions to one or more of its IAM users to manage company A's resources.

Requirements

- Company B wants to authorize its employees (IAM users) to manage the delegated resources of company A.
- If company A creates multiple agencies for company B, company B can allocate the agencies to different employees. This will allow employees to only manage specific agencies.

Solution

- Account B creates users on the IAM console, and grants the permissions (including Agent Operator) required for managing delegated resources to the users.
- Account B creates a custom policy and grants permissions defined in this policy only to one agency. In this way, users with this policy attached only have permissions to manage that agency.

Procedure

Account B performs the following procedure to authorize IAM users to manage resources of specific agencies. After authorization, the IAM users of account B can switch their roles to account A to manage account A's resources. To do this, account B needs to have obtained the account (HUAWEI ID), agency name, and agency ID of the delegating party.

Step 1 Create a user group and grant permissions to it.

1. In the navigation pane, choose **User Groups**.

2. On the **User Groups** page, click **Create User Group**.

3. Enter the user group name, for example, **Agency Management**.

4. Click **OK**.

   The user group is displayed in the user group list.

5. In the row containing the target user group, click **Authorize**.

   📖 **NOTE**

   – To authorize a user to manage only the resources of a specific agency, perform the following steps.

   – To authorize a user to manage the resources of all agencies, go to the **next step**.

   a. On the **Select Policy/Role** page, click **Create Policy** in the upper right.

   b. Enter a policy name, for example, **Agency 1 for Managing Company A**.

   c. Select **JSON** for **Policy View**.

   d. In the **Policy Content** area, enter the following content:
   ```
   {
       "Version": "1.1",
       "Statement": [
           {
               "Action": [
                   "iam:agencies:assume"
               ],
               "Resource": {
                   "uri": [
                       "/iam/agencies/b36b1258b5dc41a4aa8255508xxx..."
                   ]
               },
               "Effect": "Allow"
           }
       ]
   }
   ```

   📖 **NOTE**

   Replace *b36b1258b5dc41a4aa8255508xxx...* with the agency ID obtained from a delegating party. Do not make any other changes.

   e. Click **Next**.

6. Select the **Agency 1 for Managing Company A** agency created in the **previous step** or the **Agent Operator** role.

   📖 **NOTE**

   – The custom policy allows the user only to manage resources of a specific agency ID.

   – The **Agent Operator** role allows the user to manage the resources of all agencies.

7. Specify the authorization scope.

8. Click **OK**.

Step 2 Create a user and add the user to the user group.

1. In the navigation pane, choose **Users**.

2. On the **Users** page, click **Create User**.

3. On the **Create User** page, enter a username and email address.

4. For **Access Type**, select **Management console access**.

5. For **Credential Type**, select **Set by user**.

6. Enable login protection, select a verification mode, and click **Next**.

7. Select the user group **Agency Management** created in **2** and click **Create**.

Step 3 Switch the role.

1. Log in to Huawei Cloud as the user created in **Step 2**. For more information, see **Logging In as an IAM User**.

2. Click the username in the upper right corner, and choose **Switch Role**.

Figure 5-1 Switching roles
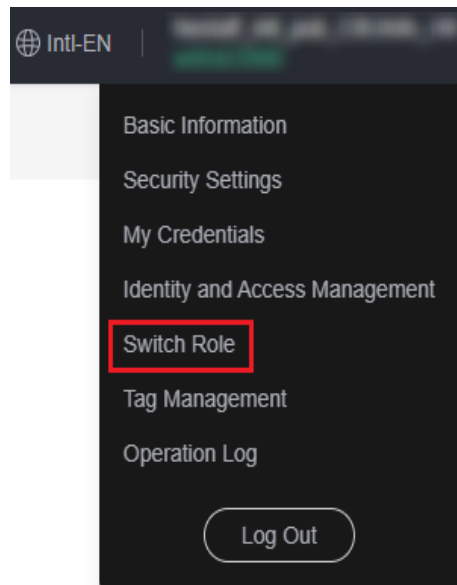
3. Enter the account name of the delegating party. The agency created by the delegating party is displayed automatically.

📖 **NOTE**

If an agency other than the agencies created by the delegating party is displayed, a message is displayed indicating that you do not have access permissions. Select the correct agency in the **Agency Name** drop-down list box.

4. Click **OK** to switch to the delegating account.

----End

5.2 Configuring an Agency for an ECS

You can create an agency to delegate access to services offered by Huawei Cloud. This example shows how to create an agency and delegate permissions to Huawei Cloud Elastic Cloud Server (ECS), a scalable, on-demand provisioning cloud server.

Application Scenarios

Applications running on an ECS must provide security credentials to access Huawei Cloud services.

Applications can use long-term (such as username and password) or temporary credentials for access. Temporary credentials are more secure because they have a

limited lifetime and are automatically rotated. To use temporary credentials to access Huawei Cloud resources, configure an agency with permissions delegated to the ECS where the applications are running, and the applications will get the temporary credential of the agency.

Figure 5-2 Obtaining a temporary credential
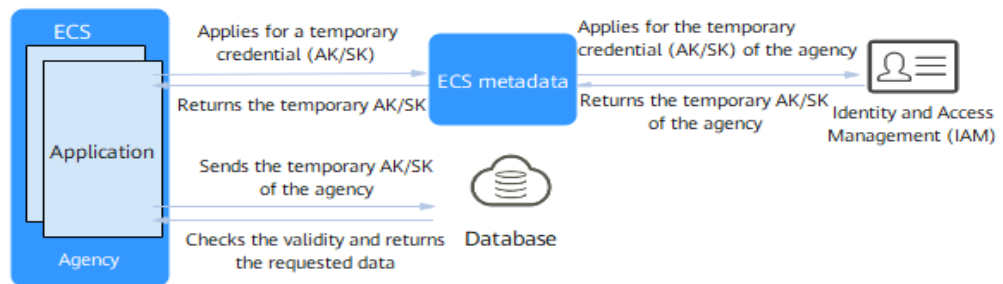
For example, configure an agency for the ECS to enable the applications running on an ECS to use a temporary credential to access a Huawei Cloud database. The ECS sends a request to get a temporary credential (AK/SK) from ECS metadata. The ECS metadata gets a temporary AK/SK of the agency from IAM and then returns the AK/SK to the ECS. The database allows access only after checking that the temporary credential sent from the ECS is valid.

Solution

Create an agency on the IAM console and specify the permissions and scope to delegate permissions to ECS. Configure the agency for the ECS where applications are running. Then the ECS will get a temporary credential of the agency to access resources based on the permissions assigned.

1. Create an agency with permissions delegated to ECS and select the permissions and scope for the agency.
2. Configure the created agency for the ECS. Only one agency can be configured for an ECS.
3. Obtain the temporary credential (AK/SK) of the agency to allow applications running on the ECS to access other Huawei Cloud resources based on the assigned permissions in the authorized scope.

Figure 5-3 ECS agency
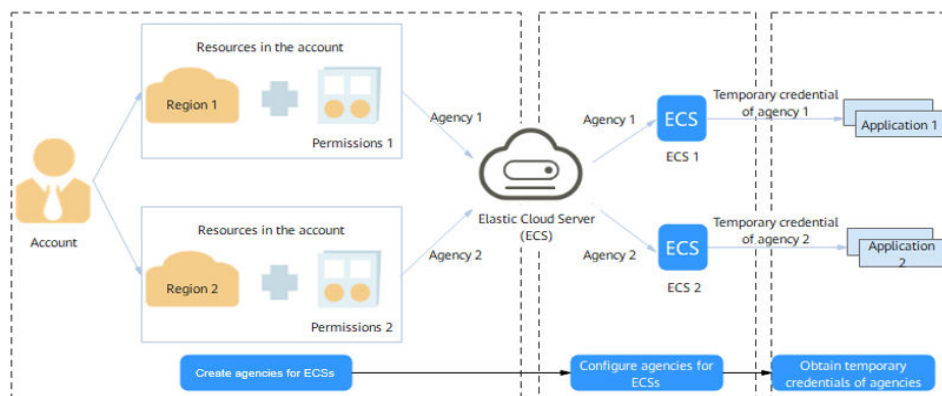
Process Flow

Figure 5-4 Flowchart
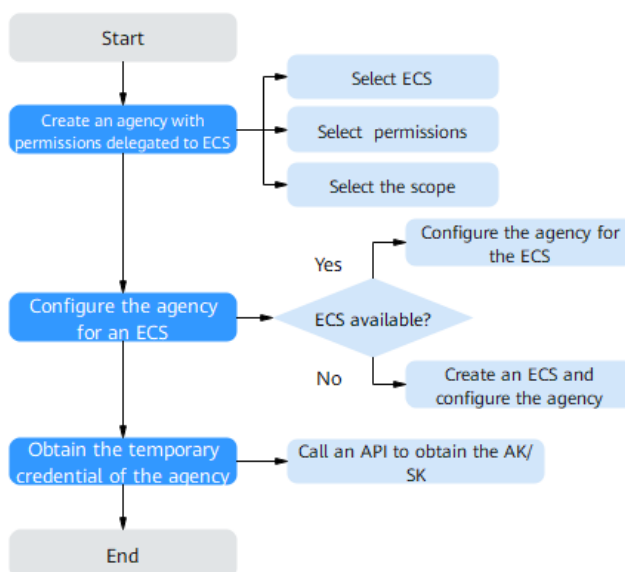
Procedure

To allow applications running on an ECS to access resources in other Huawei Cloud services, do as follows:

Step 1 **Create an agency for ECS as the administrator.**

1. Log in to the IAM console.

2. On the IAM console, choose **Agencies** from the navigation pane on the left, and click **Create Agency** on the displayed page.

3.   Enter an agency name.

4.   Select **Cloud service** for **Agency Type** and **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)** for **Cloud Service**.

Figure 5-5 Creating an agency

5.   Select a validity period.

6.   (Optional) Enter a description for the agency to facilitate identification.

7.   Click **Done**.

8.   In the displayed dialog box, click **Authorize**.

9.   Select the permissions to be assigned to the agency, click **Next**, and specify the authorization scope.

10. Click **OK**.

Step 2 **Configure the agency for the ECS as the administrator or an IAM user with ECS permissions.**

●   If there are no available ECSs, create one by referring to **Purchasing a Custom ECS**. When configuring **advanced settings**, select the agency created in step **Step 1** from the drop-down list.
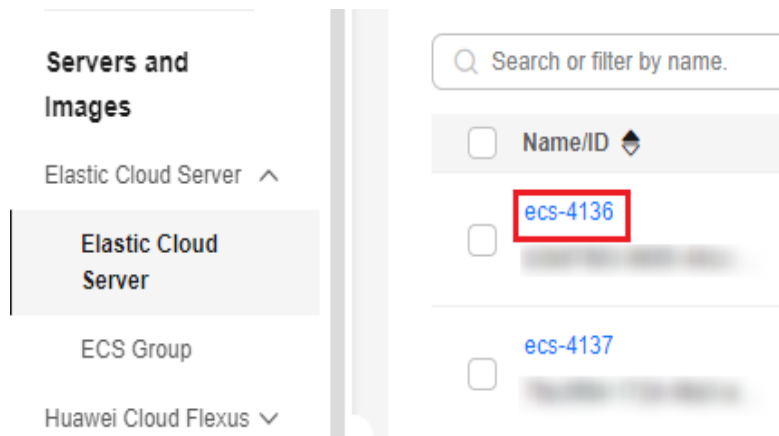
Figure 5-6 Selecting an agency

●   If there are available ECSs, configure the created agency for an ECS as follows:
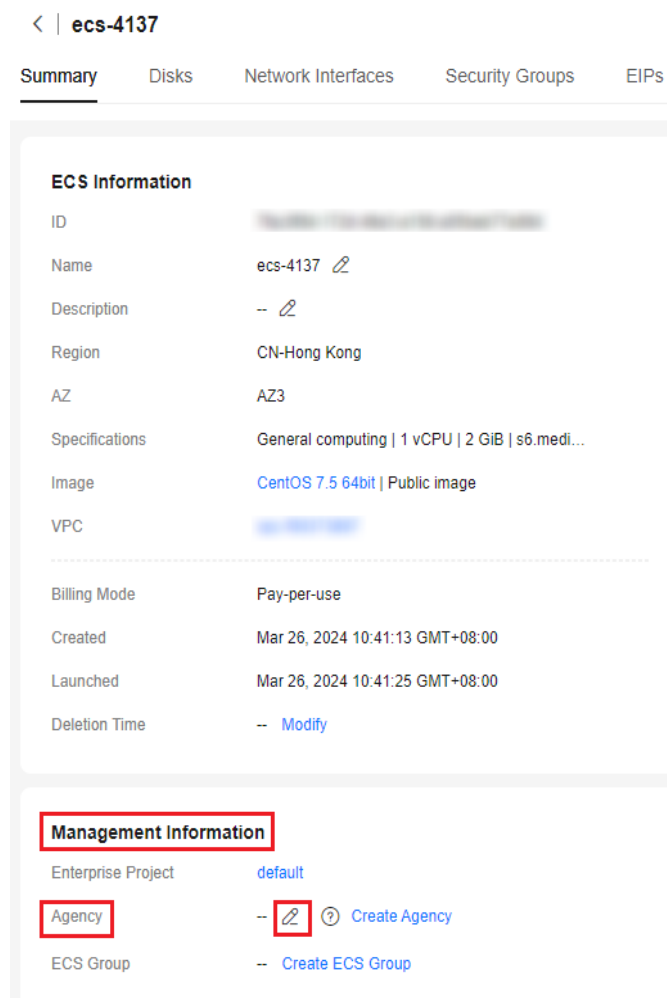
1. On the ECS console, click an ECS for which you want to configure the agency.
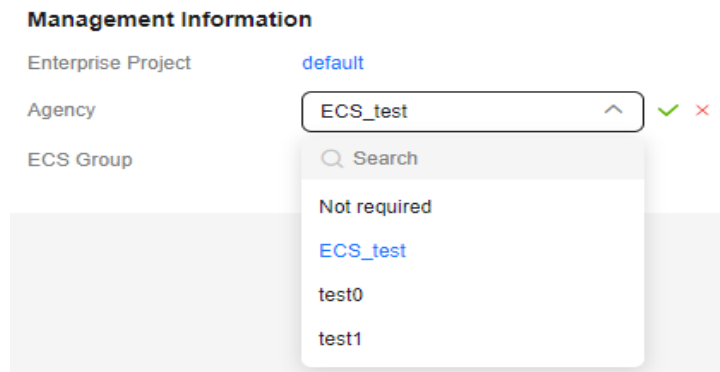
    Figure 5-7 Clicking the ECS name

2. In the **Management Information** area, click ✎ .

    Figure 5-8 Selecting an agency for the ECS

3. Select the agency created in **Step 1** from the drop-down list.

Figure 5-9 Selecting an agency

4. Click ✓ to complete the configuration.

Step 3 **Enable applications on the ECS to get a temporary credential.**

Configure applications running on the ECS to call API **Security Key (OpenStack Metadata API)** to obtain the temporary credential (AK/SK) of the agency to access other Huawei Cloud services.

● URI

/openstack/latest/securitykey

● Method

Supports GET requests.

● Example

Linux:

curl http://169.254.169.254/openstack/latest/securitykey

Windows:

Invoke-RestMethod http://169.254.169.254/openstack/latest/securitykey

📖 NOTE

   ECS automatically rotates temporary credentials to ensure that they are secure and valid.

----End

6 Cross-Region Permissions Assignment (Original Multi-Project Management)

6.1 Scenario

Company A is an enterprise user of Huawei Cloud, and it has multiple project teams that require different resources and personnel. This section presents the best practice for multi-project management to address company A's requirements.

Requirements

- **Requirement 1**: Company A can purchase multiple types of resources in **CN-Hong Kong** and **AP-Singapore** for two project teams. Resources of the two project teams need to be isolated from each other. Access to specific cloud services needs to be authorized, for example, only authorized IAM users can access and use ECS.

- **Requirement 2**: Each member of the project teams can access only the resources of the project team to which the member belongs, and only has the permissions required to complete tasks.

- **Requirement 3**: Each project team makes payments only for the resources used by its members, and the project expenditures are clear.

Solution

- **Solution to requirement 1**: Enterprise Management (EPS) and Identity and Access Management (IAM) are two cloud services of Huawei Cloud that can isolate resources between projects. However, the implementation logic and functions of the two services are different.

  - **Enterprise Management**: You can create enterprise projects to group and manage resources across regions. Resources in enterprise projects are logically isolated from each other. **Each enterprise project can contain resources of multiple regions**, and resources can be added to or removed from enterprise projects. Specified resources of certain services, for example, a specific ECS, can be added to or removed from enterprise projects.

– **IAM**: IAM projects group and physically isolate resources in a region, **and each IAM project can only contain resources in the same region.**

In conclusion, Enterprise Management provides more flexible cross-region resource isolation between projects than IAM. Therefore, it is recommended that company A use Enterprise Management to manage project resources. The solutions to the following requirements are proposed using the Enterprise Management service. For details about the two services, see **What Are the Differences Between IAM and Enterprise Management?**

● **Solution to requirement 2**: In IAM, company A creates IAM users for employees and adds the IAM users to different groups. In Enterprise Management, company A adds the user groups to the enterprise projects created to address **Requirement 1** and assigns required resource access permissions (see **Table 6-1**) to each user group.

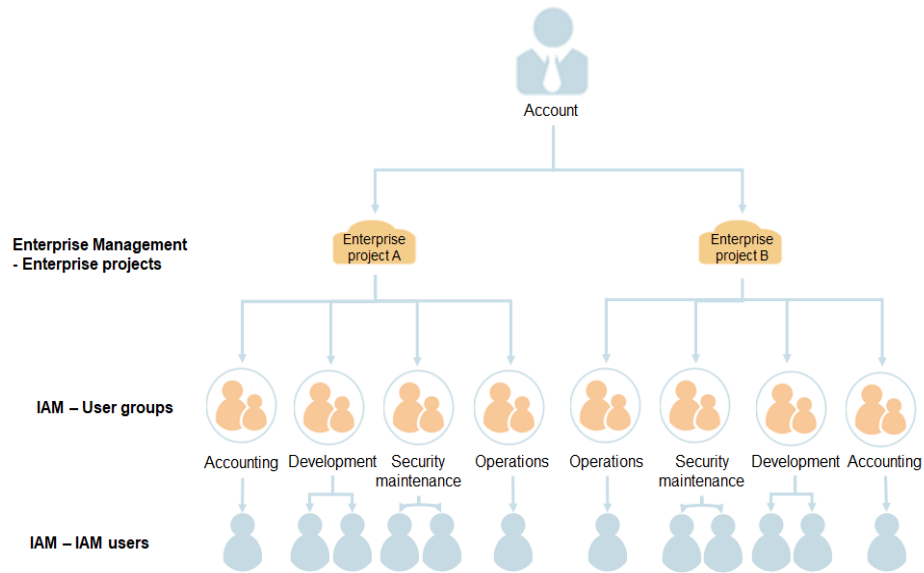**Figure 6-1** Personnel management model of company A

Table 6-1 User group permissions in company A

User Group	Responsibility	Permissions	Description
Accounting team	Project expenditure management	Enterprise Project BSS FullAccess	Permissions for accounting management of enterprise projects
Development team	Project development	ECS FullAccess	Full permissions for Elastic Cloud Server (ECS)
		OBS FullAccess	Full permissions for Object Storage Service (OBS)
		ELB FullAccess	Full permissions for Elastic Load Balance (ELB)

| User Group	Responsibility	Permissions	Description
Security maintenance team	Security O&M of the project	ECS CommonOperations	Permissions for basic ECS operations
		CAD Administrator	Full permissions for Advanced Anti-DDoS (AAD)
Operations team	Overall operations of the project	EPS FullAccess	Full permissions for Enterprise Management, including modifying, enabling, disabling, and viewing enterprise projects

☐ NOTE

For details about permissions of all Huawei Cloud services, see **System-defined Permissions**.

● **Solution to requirement 3**: Company A uses Enterprise Management to manage renewals, orders, accounting, unsubscriptions, changes, and quotas of each enterprise project. For details, see **Enterprise Project Accounting Management**.

6.2 Procedure

The following figure illustrates the process of enterprise project management for addressing company A's requirements.

Figure 6-2 Enterprise project management process
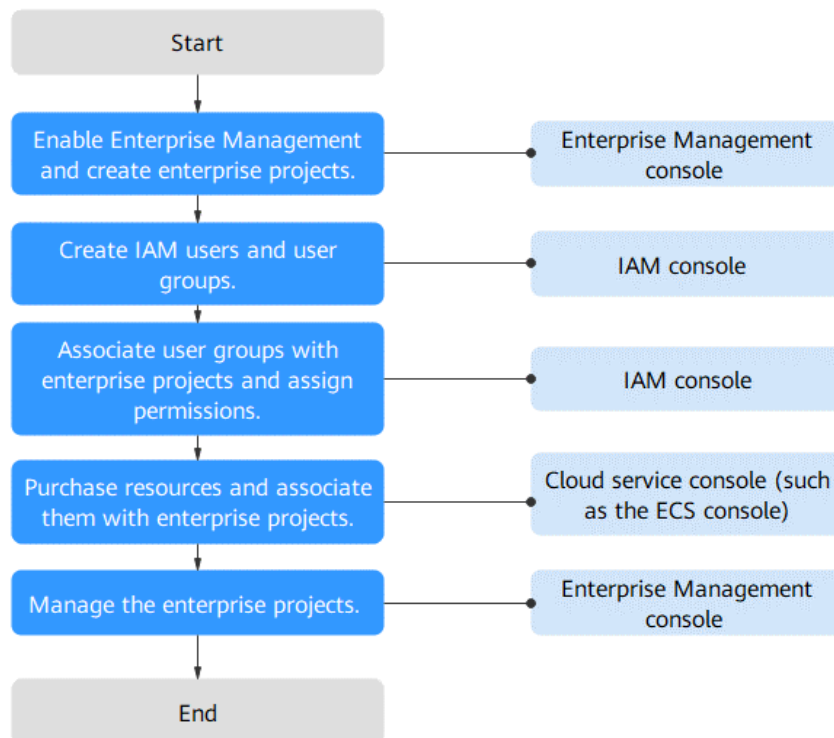
Step 1: Enable the Enterprise Management service and create enterprise projects on the Enterprise Management console.

Step 2: On the IAM console, create a user group for each functional team, create IAM users for employees, and add the users to different user groups.

Step 3: On the IAM console, assign the required permissions to each user group, and add the user group to the corresponding enterprise project. Users in the group automatically inherit its permissions.

Step 4: Purchase resources on other cloud service consoles and associate the resources with the corresponding enterprise projects.

Follow-Up Operation: Enterprise Project Management: Perform personnel, resource, and accounting management on the Enterprise Management console.

Enabling Enterprise Management and Creating Enterprise Projects

Perform the following procedure to create two enterprise projects (A and B) on the Enterprise Management console. If you have enabled Enterprise Project, go to **Step 4**.

Step 1 Log in to the Huawei Cloud console, hover over the account name in the upper right corner and choose **Basic Information**.

Step 2 On the **Basic Information** page, click **Enable Enterprise Project Function**.

Step 3 Read and agree to the *Huawei Cloud Enterprise Management Agreement*, and click **Apply Now**.

Step 4 On the Huawei Cloud management console, choose **Enterprise** > **Project Management**.

Figure 6-3 Accessing the Enterprise Project Management page
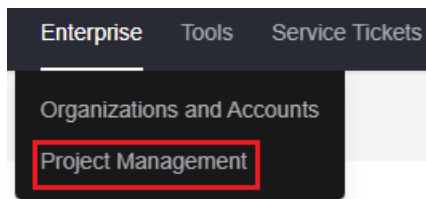
Step 5 On the **Enterprise Project Management Service** page, click **Create Enterprise Project**.

Figure 6-4 Creating an enterprise project
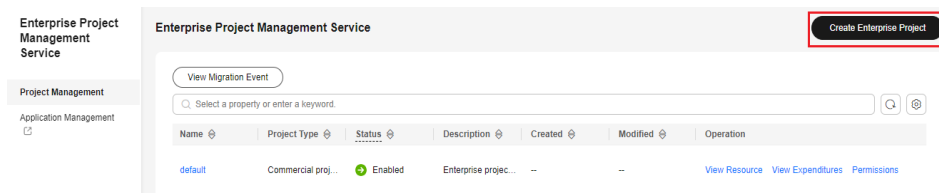
Step 6 Enter **Enterprise_Project_A** for **Name** and click **OK**.

Step 7 Repeat steps **5** to **6** to create **Enterprise_Project_B.**

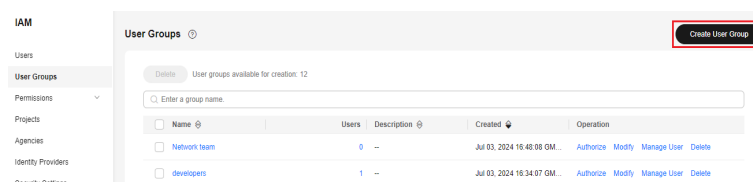The two enterprise projects are displayed on the **Enterprise Project Management Service** page.

----End

Creating IAM Users and User Groups

The following is an example procedure for creating a user group (**Enterprise Project A_Accounting**) and user (**Murphy**) and adding the user to the user group.

Step 1 Create a user group.

1. Go to Huawei Cloud management console, and choose **Service List** > **Management & Governance** > **Identity and Access Management**.

2. On the IAM console, choose **User Groups** in the navigation pane. Then click **Create User Group**.

Figure 6-5 Creating a user group

3. Set the user group name to **Enterprise Project A_Accounting** and click **OK**.

4. Repeat steps **2** to **3** to create the accounting, development, security maintenance, and operations teams for the two enterprise projects.

The user groups are displayed in the user group list.

Step 2 Create an IAM user and add the user to a user group.

1. In the navigation pane of the IAM console, choose **Users**. Then click **Create User**.

2. Specify the user details, select **access types** (see **Figure 6-6**), and click **Next**.

Figure 6-6 Creating an IAM user

3. Add user **Murphy** to the user group **Enterprise Project A_Accounting** and click **Create**.

Figure 6-7 Adding the user to a user group

4. Repeat steps **1** to **3** to create users for all employees and add the users to corresponding user groups.

    The user is displayed in the user list. You can view the IAM users of each user group on the **Users** tab page.

    ----End

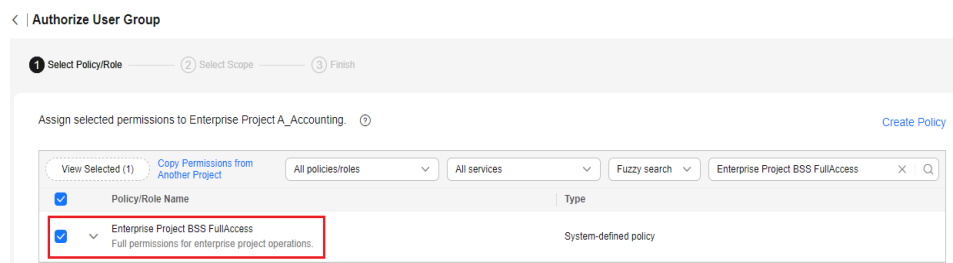## Associating User Groups with Enterprise Projects

Assign permissions to a user group and apply user group permissions to enterprise projects.

Step 1 Log in to the IAM console as an administrator.

Step 2 In the user group list, locate the row containing the target user group and click **Authorize** in the **Operation** column.

Step 3 On the displayed page, search for **Enterprise Project BSS FullAccess** in the search box, select it, and click **Next**.
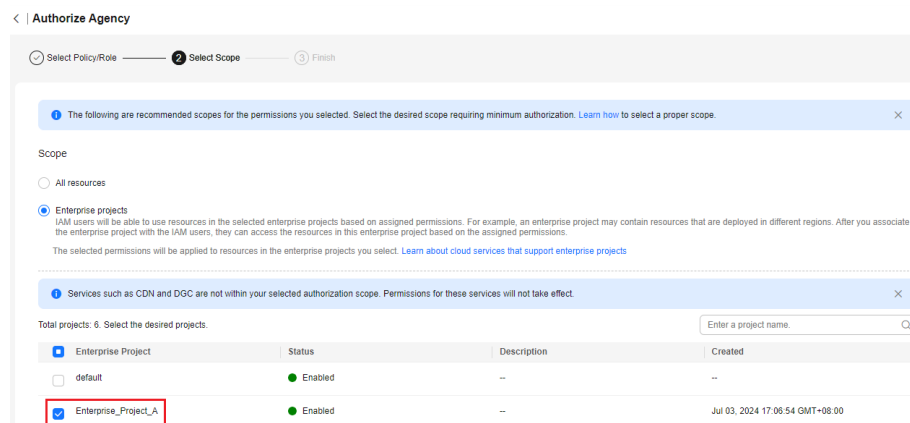
> 📖 **NOTE**
>
> You can create custom policies to supplement system-defined policies for fine-grained permissions management. For details, see **Creating a Custom Policy**.

Figure 6-8 Selecting permissions

Step 4 Select the **Enterprise projects** authorization scope.

Figure 6-9 Selecting an enterprise project

Step 5 In the enterprise project list, select **Enterprise Project A**.

**Step 6** Click **OK**.

----End

Purchasing Resources and Associating Them with Enterprise Projects

The following is an example procedure for purchasing an ECS and associating it with enterprise project A.

Step 1 Log in to the Huawei Cloud management console, click ☰ in the upper left corner, and choose **Compute** > **Elastic Cloud Server**.
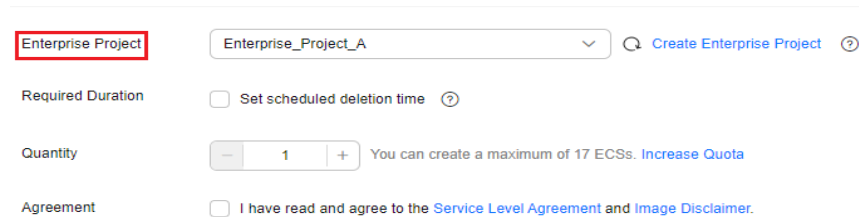
Step 2 Click **Buy ECS** in the upper right corner.

Figure 6-10 Buying an ECS
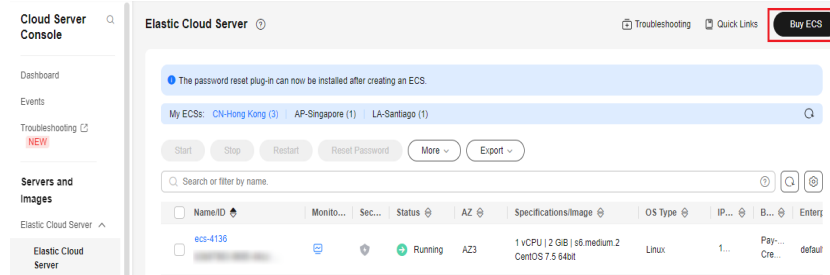
Step 3 **Specify the ECS details** and select **Enterprise_Project_A** from the **Enterprise Project** drop-down list.

Figure 6-11 Selecting an enterprise project

Step 4 Click **Next** in the lower right corner to view the resource details and submit the order.

Step 5 Repeat **Step 1** to **Step 4** to purchase required resources for the two enterprise projects.

To view the purchased resources, go to the Enterprise Management console and click **View Resource** in the row that contains enterprise project A or B.

📖 **NOTE**

- Currently, Enterprise Management only supports **specific Huawei Cloud services**.
- If you have already purchased required resources, you can directly associate them with the two enterprise projects. For details, see **Adding Resources to an Enterprise Project**.

----End

Follow-Up Operation: Enterprise Project Management

After completing the preceding steps, you can manage your enterprise projects on the **Enterprise** > **Project Management** > **Enterprise Project Management Service** page.

- **Resource management**: Click **View Resource** to view the existing resources of an enterprise project and **add more resources to the enterprise project**.

- **Personnel management**: Choose **More** > **Permissions** to go to the IAM console to view the users and user groups associated with an enterprise project, and modify the users, user groups and their permissions for the enterprise project. For details, see **Personnel Management**.

- **Accounting management**: Click **View Expenditures** to view the orders and bills and manage renewals of an enterprise project. For details, see **Enterprise Project Accounting Management**.