IAM 5.0 Best Practices

Issue 01

Date 2025-11-07

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 Security Best Practices in IAM

Use IAM Identity Center to Centrally Manage Human-Machine Users with Identity Federation

Huawei Cloud users can be administrators, developers, and application users (such as business analysts and data analysts). They use the CLI, console, or client applications to access Huawei Cloud. They are members of your enterprise or organization. They can also be users outside the enterprise or organization. They must have identity credentials to access Huawei Cloud. You are advised to use **IAM Identity Center** to manage these users. The benefits are as follows:

- Centrally manage users: Any changes of the enterprise or organization members can be maintained only in one system.
- Centrally manage user credentials: You do not have to create or maintain passwords in different systems.
- Reduce the number of identity systems: You can manage user identities from an identity provider.
- Simplify audit: A single identity source makes audit easy.

Use Temporary Access Keys with IAM Agencies or Trust Agencies to Allow Machine-Machine Users to Access Huawei Cloud

Using temporary access keys is a security best practice because they have a limited lifetime and automatically expire. You do not need to rotate them periodically or delete them when they are no longer needed. You are advised to use IAM agencies or trust agencies to issue temporary credentials rather than permanent access keys of IAM users to machine-machine accounts.

Do Not Write Access Keys into Code

If you use APIs, CLI, 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 Method

You can access Huawei Cloud in different ways. For IAM users created on the new IAM console, the access method depends on the credential types of the users. If you set a console password when creating an IAM user, the IAM user can access Huawei Cloud through the console. If you create an access key for an IAM user, the IAM user has programmatic access to Huawei Cloud. For IAM users created on the old IAM console, you can specify the access type when creating an IAM user or choose **More** > **Security Settings** in the user list and set the password or access keys after the user is created.

Enable 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 for your account and its IAM users. After MFA is enabled, you need to enter verification codes after your username and password are authenticated. Virtual MFA devices, together with your username and password, ensure the security of your account and resources.

You can choose either a virtual MFA device or a security key. A virtual MFA device is an application that generates 6-digit verification codes. MFA applications can run on mobile devices (including smartphones) and are easy to use. Security keys are a two-factor authentication method based on the Fast Identity Online (FIDO) protocol. Currently, Huawei Cloud supports FIDO-based devices and Windows Hello security keys.

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 a critical operation, such as deleting a resource or generating an access key, you and users need to provide the password and a verification code to proceed with the operation.

Periodically Change Your Identity Credentials

Periodically changing your password and access keys can prevent risks caused by their accidental disclosure or loss. You can use the following methods:

- Set a password validity period to require you and your users to rotate passwords. IAM will start to display a prompt 15 days before the passwords expire.

- Create two access keys and rotate them in your applications. For example, use access key 1 for a period, and then use access key 2 for the next period. Then delete access key 1, generate another access key (access key 3), and rotate access key 2 and access key 3 periodically. In this way, two access keys are continuously rotated to ensure secure login.

Delete Unnecessary Identity Credentials

For users who only need to use the console, you are advised not to create access keys for them and delete the 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.

Enable CTS

You can use Cloud Trace Service (CTS) to collect, store, and query key IAM operations for security analysis, compliance audit, resource tracking, and fault locating. It is recommended that you enable CTS to record key IAM operations, such as creating and deleting users.

Comply with Best Practices to Protect Account Credentials

Your account has all the permissions required to access resources and make payments for the usage of resources. Safeguard your account credentials the same way you would protect other sensitive personal information.

- Do not create access keys for the accounts.

  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. They are supplementary to passwords and used for programmatic requests with development tools. To enhance account security, you are advised to only use the password to log in to the console. Do not create access keys for your account to eliminate information security risks posed by access key loss or disclosure.

- Secure your account credentials to prevent unauthorized use.

  Safeguard your account credentials and use them only for the tasks that require them. Strictly control the scope that requires account credentials for authentication. Do not disclose your password, MFA, and access keys.

- Use strong passwords to enhance access protection.

  You are advised to use password tools to generate strong passwords. Do not set the password to your account name or email address.

- Enable MFA.

  It is strongly recommended to enable MFA for the account.

- Use multi-person approval for account login.

  To ensure that nobody can access both the password and MFA of the account, use multi-person approval. For example, you can set one group of administrators with access to the password and another group of administrators with access to MFA. One member from each group must come together to sign in as the account.

- Monitor the account permissions and usage.

  Use CTS to monitor the account usage. If any exception is detected, perform security audit and prevention in a timely manner.

Grant Least Privilege

As a security best practice, grant only permissions required to perform specific tasks. You can achieve this by using the IAM system-defined permissions or custom policies and identity policies. The principle of least privilege 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 or identity policies to minimize impact due to accidental access key disclosure or loss.

- Create IAM users for administrators and applications, respectively.
- For IAM users used by administrators, use an identity provider to provide federated access to Huawei Cloud accounts and store the passwords in the enterprise's offline identity system.
- For IAM users used by applications, only grant the permissions needed to call specific APIs and disable console login (to avoid saving the password).
- Do not grant permission to download or delete important data assets, or only grant these permissions to a few important IAM users (or federated users). Do not share the passwords of these users to minimize the impact of password disclosure or loss.

Use Conditions in IAM Policies or Identity Policies to Further Restrict Access

You can use IAM policies or identity policies to further restrict access. For example, you can write a policy or identity policy to only allow specific IAM users to perform specific operations. For more information, see **IAM Permissions Management**.

Delete or Do Not Generate Root User Access Keys

For account security, do not generate an access key for the root user unless necessary (which is rarely the case). The best practice is to create an IAM Identity Center user to manage routine tasks. For details about how to create IAM Identity Center users for management, see **Getting Started**.

If you have been using the access key of an account's root user, you are advised to locate this access key in your application, replace it with the IAM user's access key, and then disable and remove the root user's access key.

Control the Use of Access Keys

It is recommended to use **temporary security credentials** to access Huawei Cloud for running workloads. If permanent access keys are required, it is recommended to follow the principle of least privilege (PoLP) and enable MFA when granting permissions to IAM users with permanent access keys.

For example, if you choose to use an IAM user's permanent access key to run the workloads for short-term tests, you are advised to use condition keys to restrict

user permissions. In this case, you can create a temporary identity policy and attach it to the IAM user so that the user's permissions will expire after a specified period of time. If you are running a workload from a secure network, you can use an identity policy that restricts the access based on IP addresses.

- **Configure a Temporary Policy for an IAM User.**
  a. Log in to the **new IAM console** as an administrator.
  b. In the navigation pane, choose **Identity Policies**.
  c. In the upper right corner, click **Create Identity Policy**. On the displayed page, enter the policy name and set **Policy View** to **JSON**.
  d. In the **Policy Content** area, enter the following policy and replace the value of the condition key **g:CurrentTime** with the required expiration time.

```
{
   "Version": "5.0",
   "Statement": [{
      "Effect": "Deny",
      "Action": [
         "*"
      ],
      "Condition": {
         "DateGreaterThan": {
            "g:CurrentTime": [
               "2025-07-15T08:53:13Z"
            ]
         }
      }
   }]
}
```

  This policy denies all operations on all resources after the specified date. The **DateGreaterThan** operator is used to check whether the current time is later than the specified time.
  e. Click **OK**. The **Identity Policies** page is displayed. Search for the identity policy you created in the search box, select the policy, and click **Attach** to attach the policy to the specified IAM user.

  Then, the identity policy is displayed on the **Permissions** tab of the user. If the current time reaches or exceeds the time specified in the identity policy, the user can no longer access Huawei Cloud resources. Ensure that developers are aware of the expiration dates you set for user permissions.

- **Configure a Policy to Deny Access Based on the IP Address of an IAM User**
  a. Log in to the **new IAM console** as an administrator.
  b. In the navigation pane, choose **Identity Policies**.
  c. In the upper right corner, click **Create Identity Policy**. On the displayed page, enter the policy name and set **Policy View** to **JSON**.
  d. In the **Policy Content** area, copy the following IAM policy to the JSON editor and change the public IP address or range as required. You can use a slash (/) to specify a single IP address or an IP address range. For more information, see **g:SourceIp**.

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

```
        "Resource": [
            "*"
        ],
        "Condition": {
            "NotIpAddress": {
                "g:SourceIp": [
                    "xx.xx.xx.0/32"
                ]
            },
            "BoolIfExists": {
                "g:ViaService": [
                    "false"
                ]
            }
        }
    },
    {
        "Effect": "Deny",
        "Action": [
            "*"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "NotIpAddress": {
                "g:SourceIp": [
                    "xx.xx.xx.0/32"
                ]
            },
            "StringEquals": {
                "g:CalledViaFirst": "service.console",
                "g:CalledViaLast": "service.console"
            }
        }
    }
  ]
}
```

This policy denies all operations on all resources except the specified IP addresses. The **NotIpAddress** operator specifies all IP addresses except the specified IP addresses or range.

e. Click **OK**. The **Identity Policies** page is displayed. Search for the identity policy you created in the search box, select the policy, and click **Attach** to attach the policy to the specified IAM user.

You can also apply the following policy as a service control policy (SCP) to multiple Huawei Cloud accounts. You are advised to use the condition key **g:PrincipalUrn** to apply the policy only to IAM users in the accounts restricted by the SCP.

```
{
  "Version": "5.0",
  "Statement": [{
        "Effect": "Deny",
        "Action": [
            "iam:*:*"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "NotIpAddress": {
                "g:SourceIp": [
                    "xx.xx.xx.0/32"
                ]
            },
            "BoolIfExists": {
```

```
                "g:ViaService": [
                    "false"
                ]
            },
            "StringMatch": {
                "g:PrincipalUrn": [
                    "iam::<account-id>:user:<user-name>"
                ]
            }
        }
    },
    {
        "Effect": "Deny",
        "Action": [
            "iam:*:*"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "NotIpAddress": {
                "g:SourceIp": [
                    "xx.xx.xx.0/32"
                ]
            },
            "StringEquals": {
                "g:CalledViaFirst": "service.console",
                "g:CalledViaLast": "service.console"
            },
            "StringMatch": {
                "g:PrincipalUrn": [
                    "iam::<account-id>:user:<user-name>"
                ]
            }
        }
    }
  ]
}
```

2 Best Practices for the Root User

Your account registered with Huawei Cloud has the highest operation permissions on all resources in this account. This identity is called the root user. You can log in to Huawei Cloud using the account name and password, or using the account name, username with the same account name, and password. You need to safeguard your root user credentials. If they are leaked, all resources and data in the account will be affected. When you register an account, we strongly recommend that you create a user and add it to the admin user group. This user can then manage other identities and assign permissions. Do not access the root user unless you have a task that requires root user credentials.

Secure the Root User's Credentials

To help prevent unauthorized use, do not share the root user's credentials, including the password, access keys, and MFA device and use them only when necessary.

Set a Strong Password for the Root User

We recommend that you set a strong password for the root user that meets the following example conditions:

- It must contain at least 8 characters.
- It must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters.
- It must be distinct from your account name or email address.

Secure Your Root User Login with MFA

Because the root user has the highest permissions for all resources in your account, it is crucial to add an MFA device for the root user as a secondary authentication factor.

- If your account is a Huawei Cloud account (not a HUAWEI ID), you can add an MFA device by following these steps to enable login protection automatically: On the IAM console, choose **Users** > **Root User** (the enterprise administrative user). On the displayed page, click the **Security Settings** tab, and then click **Add MFA Device** in the **Multi-Factor Authentication (MFA)** area. Huawei Cloud supports only virtual MFA and security keys based on the

FIDO protocol and Windows Hello as the secondary authentication factor for the root user.

- If your Huawei Cloud account has been upgraded to a HUAWEI ID, you cannot bind an MFA device on the security settings page. Instead, go to the HUAWEI ID account center, choose **Account & security**, locate **Two-step verification** in the **Security verification** area, and click **ENABLE**. Then, enter the verification information to enable login protection. Only the mobile number, email address, and virtual MFA can be used as the secondary authentication method for the root user of a HUAWEI ID.

Use Multi-Person Approval for Root User Login

To strengthen security, we recommend you assign the root user's MFA device and password to different persons. This ensures that each login of the root user is approved by multiple persons.

Do Not Create Access Keys for the Root User

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) of the account root user are account credentials and they have the same effect. Passwords are mandatory and used for console login. Access keys are optional. They are supplementary to passwords and used for programmatic requests with development tools. To enhance account security, you are advised to only use the password to log in to the console. Do not create access keys for the root user to prevent risks from access key leakage.

Secure the Root Users of the Management Account and Member Accounts in an Organization

When you use Organizations to manage multiple accounts, you need to take the preceding measures to secure the root users of the management account and member accounts in the organization.

Restrict Root User Actions Using SCPs in Organizations

You can apply an SCP in Organizations to restrict access to the root user. For example, you can deny all root user actions in your member accounts on Elastic Cloud Server (ECS) instances. For details, see **Example SCPs**.

Automatically Evaluate the Compliance of Root User Settings

The Config service checks the compliance of the root user settings. You can use Config to check whether **the root user has available access keys** and whether **the root user has MFA enabled**.

If you have any security concerns regarding the root user, submit a service ticket on the official website or call the Huawei Cloud customer service at 4000-955-988 or 950808.

3 Assigning Permissions to O&M Personnel Using IAM

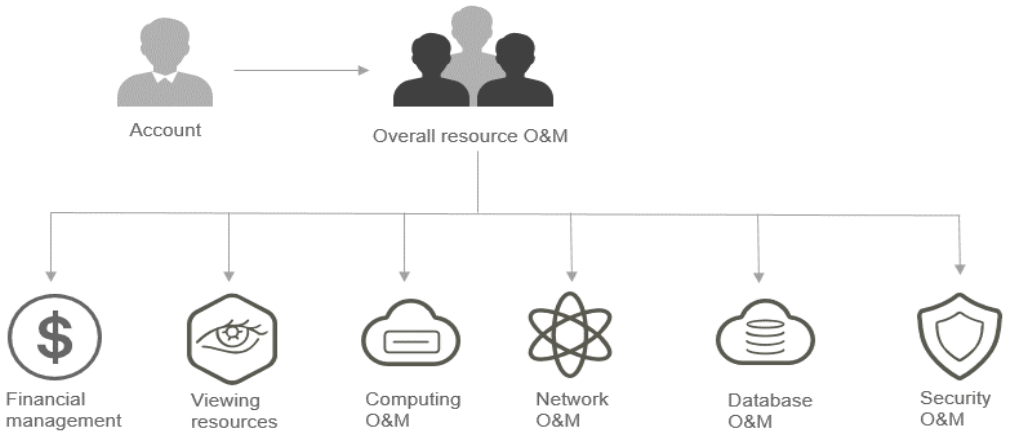
Overview

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 identity policies to set permissions for multiple O&M personnel.

Resource Planning

Based on the different responsibilities of employees in the company, employees are grouped into the following seven teams.

Figure 3-1 Permissions management model



- Resource O&M team: manages all resources of the company.
- Accounting management team: manages accounting affairs of the company.
- Resource monitoring team: views and monitors the resource usage.
- Computing O&M team: is responsible for the computing domain O&M.

- Network O&M team: is responsible for the network domain O&M.
- Database O&M team: is responsible for the database domain O&M.
- Security O&M team: is responsible for the security domain O&M.

You can assign different permissions to different functional teams according to **Table 3-1**. In this way, the permissions of different teams are isolated and each team performs its own functions. For details about system-defined permissions of all Huawei Cloud services, see **System-defined Identity Policies**.

Table 3-1 Team permissions

Functional team	Required Policy	Description
Resource O&M team	AdministratorAccessPolicy	Full permissions for all services.
Accounting management team	BILLINGFullAccessPolicy	Full permissions for Billing Center, Account Center, Cost Center, Enterprise Center, and Message Center.
Resource monitoring team	ReadOnlyPolicy	Read-only permissions for all services.
Computing O&M team	ECSFullPolicy	Full permissions for Elastic Cloud Server (ECS), including the permission to purchase ECS resources. Users granted only this permission cannot view the overall usage of ECS resources and other resources unless you grant them the **BSS Administrator** permission.
	CCEFullPolicy	Full permissions for Cloud Container Engine (CCE), including the permission to purchase CCE resources. Users granted only this permission cannot view the overall usage of CCE resources and other resources unless you grant them the **BSS Administrator** permission.
	ASFullPolicy	Full permissions for Auto Scaling (AS), including the permission to purchase AS resources. Users granted only this permission cannot view the overall usage of AS resources and other resources unless you grant them the **BSS Administrator** permission.

Functional team	Required Policy	Description
Network O&M team Database O&M team Security O&M team	VPCFullAccessPolicy ELBFullAccessPolicy RDSFullAccessPolicy DDSFullAccessPolicy DDMFullAccessPolicy Anti-DDoSFullAccessPolicy AADFullAccessPolicy KMSFullAccessPolicy	Full permissions for Virtual Private Cloud (VPC), including the permission to purchase VPC resources. Users granted only this permission cannot view the overall usage of VPC resources and other resources unless you grant them the **BSS Administrator** permission. Full permissions for Elastic Load Balance (ELB), including the permission to purchase ELB resources. Users granted only this permission cannot view the overall usage of ELB resources and other resources unless you grant them the **BSS Administrator** permission. Full permissions for Relational Database Service (RDS), including the permission to purchase RDS resources. Users granted only this permission cannot view the overall usage of RDS resources and other resources unless you grant them the **BSS Administrator** permission. Full permissions for Document Database Service (DDS), including the permission to purchase DDS resources. Users granted only this permission cannot view the overall usage of DDS resources and other resources unless you grant them the **BSS Administrator** permission. Full permissions for Distributed Database Middleware (DDM). Full permissions for Anti-DDoS. Full permissions for Advanced Anti-DDoS (AAD). Full permissions for Key Management Service (KMS), including the permission to purchase KMS resources. Users granted only this permission cannot view the overall usage of KMS resources and other resources unless you grant them the **BSS Administrator** permission.

Based on the division of the functional teams, resources are planned as follows.

Table 3-2 Resource planning

Resource	Resource Name	Description	Quantity
Administrator account	Company-A	Used to manage resources and permissions of the company.	1
IAM user groups	Network O&M	Functional teams are divided into seven user groups. The network O&M team is used as an example to describe how to create a user group.	1
IAM users	James and Alice	James and Alice are used as an example to describe how to create IAM users.	2
Permissions	VPC FullAccess and ELB FullAccess	According to the preceding table, two types of permissions need to be configured for the network O&M team.	2

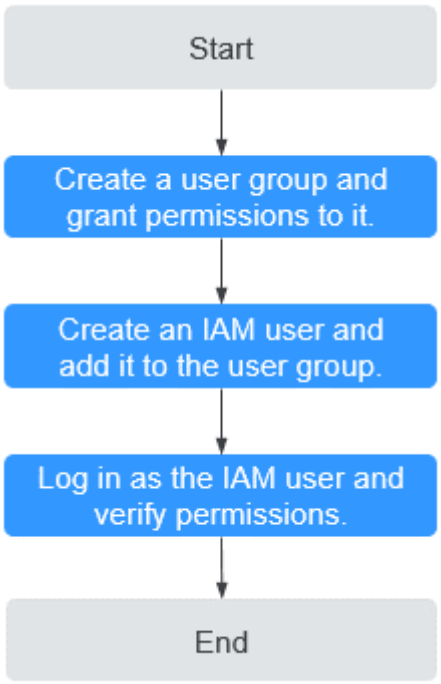
NOTE

IAM is a free service, so the best practices do not involve any expenditures.

Procedure

IAM allows you to assign permissions to users in the user groups. **Figure 3-2** shows how to grant an employee the permissions required as the network O&M owner. If you want to configure employees as other O&M owners, assign the required permissions to them based on **Table 3-1**.

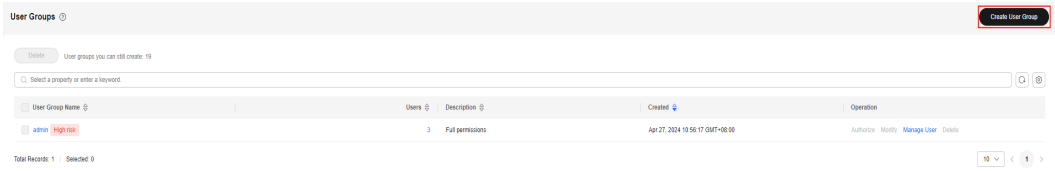
Figure 3-2 Process



Step 1: Create a User Group and Assign Permissions

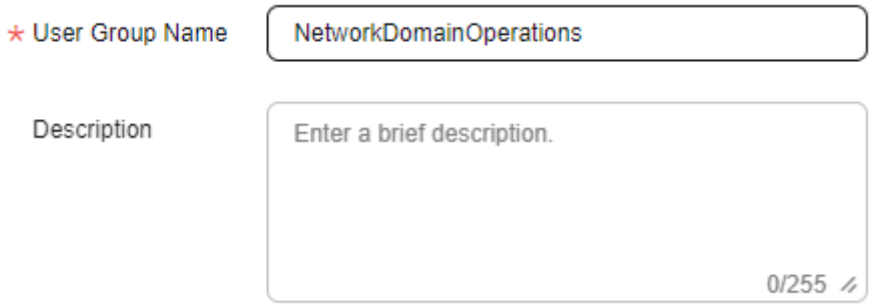
1. Log in to the Huawei Cloud management console as the administrator.
2. On the management console, hover the mouse pointer over the username in the upper right corner and then choose **Identity and Access Management**.
3. On the IAM console, choose **User Groups** in the navigation pane. Then click **Create User Group**.

   Figure 3-3 Creating a user group

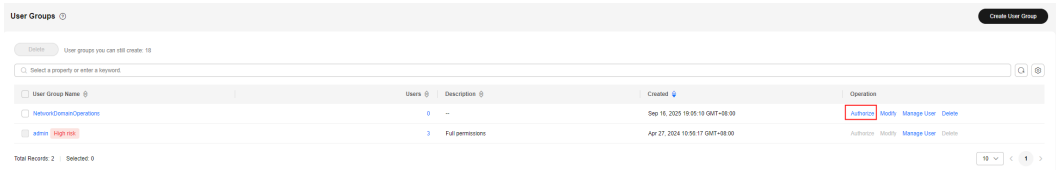
4. On the **Create User Group** page, enter the user group name **NetworkDomainOperations** and click **OK**. Only letters, digits, spaces, hyphens (-), and underscores (_) are allowed.

Figure 3-4 Entering a group name



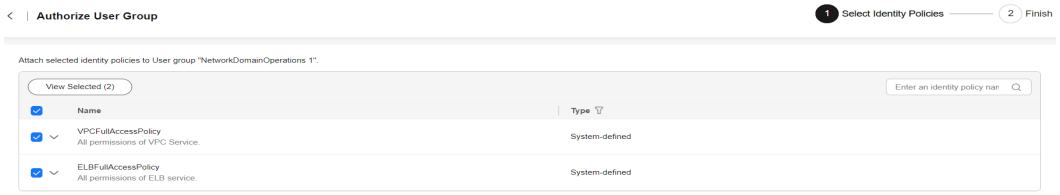
5. Locate the user group you created and click **Authorize** in the **Operation** column.

Figure 3-5 Authorizing a user group



6. Search for **VPCFullAccessPolicy** and **ELBFullAccessPolicy**, select the two policies, and click **Next**.

Figure 3-6 Selecting permissions



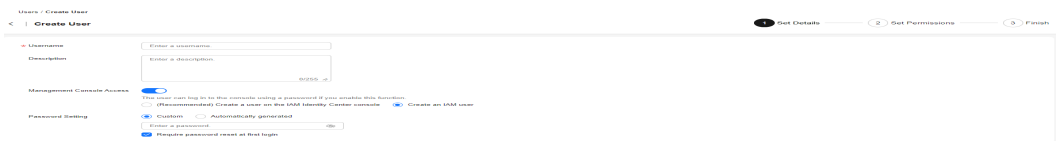
7. Click **OK**. The created user group will be displayed in the user group list.

   You can click the name of the network O&M user group and view the assigned permissions on the **Permissions** tab.

Step 2: Create an IAM User and Add It to the Group

1. Log in to the IAM console as the administrator and choose **Users** from the left navigation pane.
2. On the **Users** page, click **Create User** in the upper right corner.

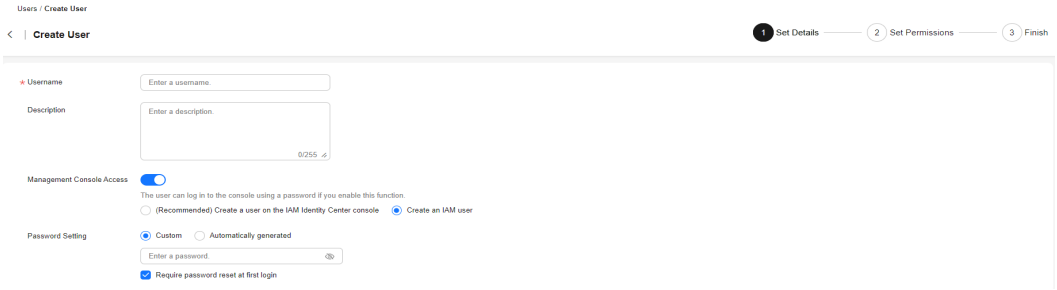
Figure 3-7 Creating a user



3. Configure basic information about users James and Alice.

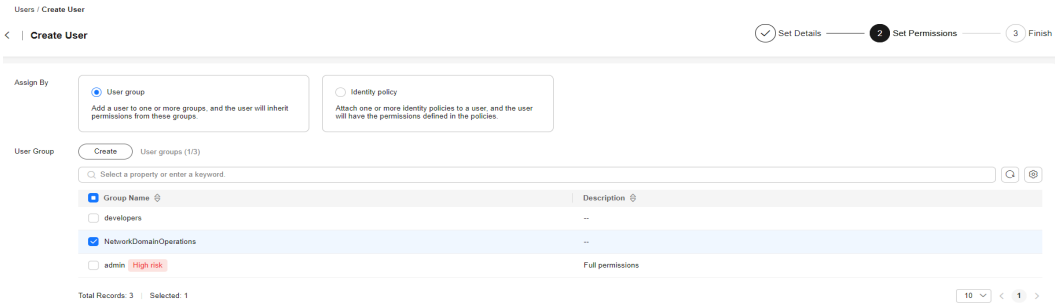
   On the **Create User** page, enter the username and description, configure the management console access, and set a password.

Figure 3-8 Setting user details



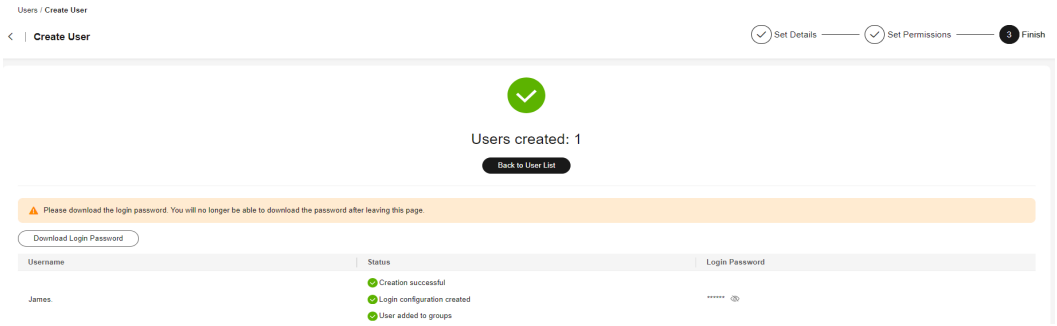
4. Click **Next** and add the IAM users James and Alice to the created network O&M user group.

Figure 3-9 Adding users to the user group



5. Click **Create User**. The IAM users are created. You can download the login password.

Figure 3-10 Users created

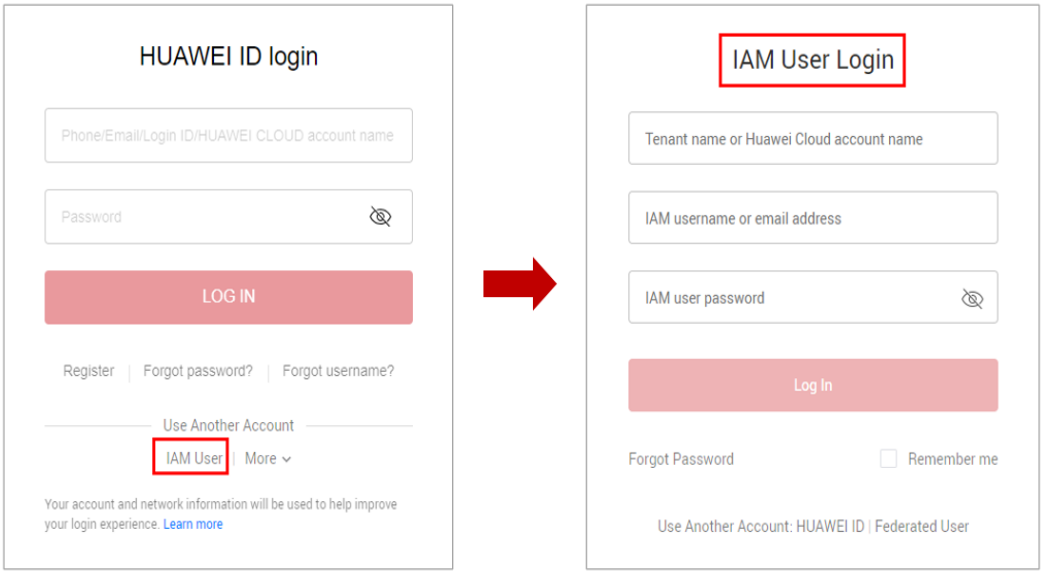


Step 3: Log In as an IAM User and Verify Permissions

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**.

1. On the Huawei Cloud login page, click **IAM User**.
2. On the **IAM User Login** page, enter the company's account name, IAM username, and password.
   - Account name: the name of the account that created the IAM user
   - Username and password: the username and password specified for the IAM user

Figure 3-11 Logging in as the IAM user



3. Log in to the Huawei Cloud management console as the IAM user.
4. Choose **Virtual Private Cloud** and then **Elastic Load Balance** from the service list to go to the homepages of these services. If you can perform management operations on the homepages, the permissions are successfully configured.
5. Choose a service other than the preceding services from the service list. If the system displays a message indicating insufficient permissions, the permissions are successfully configured.

4 Delegating Permissions Across Accounts with Trust Agencies

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 a trust agency in IAM to establish a trust relationship between the two accounts.

Requirements

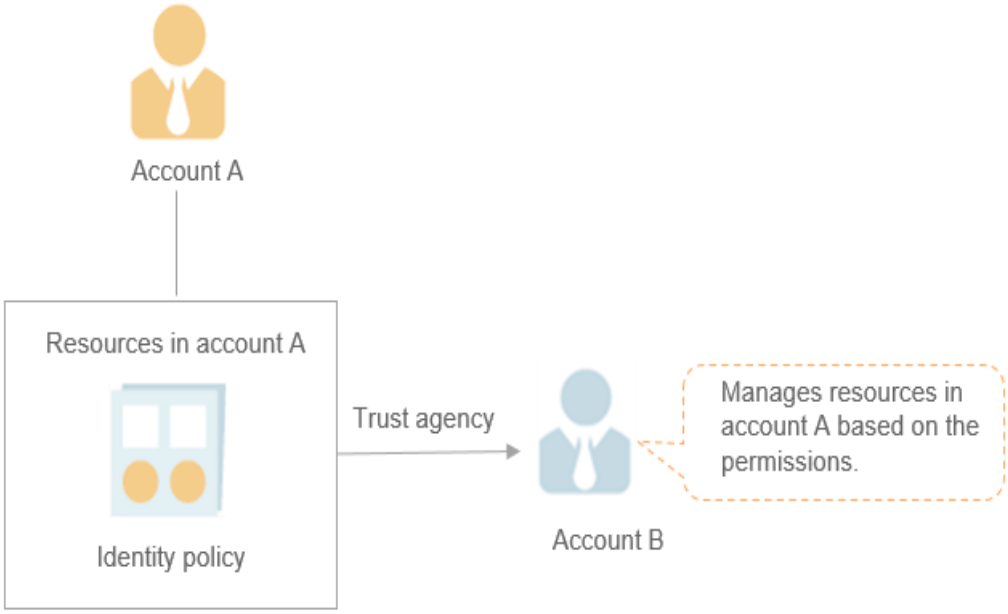
- Account A has purchased multiple types of resources on Huawei Cloud and wants to authorize account B to manage its VPC resources.
- Account B wants to authorize one or more employees (IAM users) of company B to manage account A's resources.
- Account A can modify or cancel the authorization provided to account B at any time.

Solutions

To address these requirements, the following solutions are provided:

- Account A creates a trust 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 trust agency.
- If the cooperation between the two companies changes, account A can modify or delete the trust agency anytime. Then permissions of account B and its IAM users for managing account A's resources are changed or cancelled automatically.

Figure 4-1 Cross-account authorization model



Delegating Permissions to Another Account (by the Delegating Party)

The following example describes how account A delegates account B to manage VPC resources.

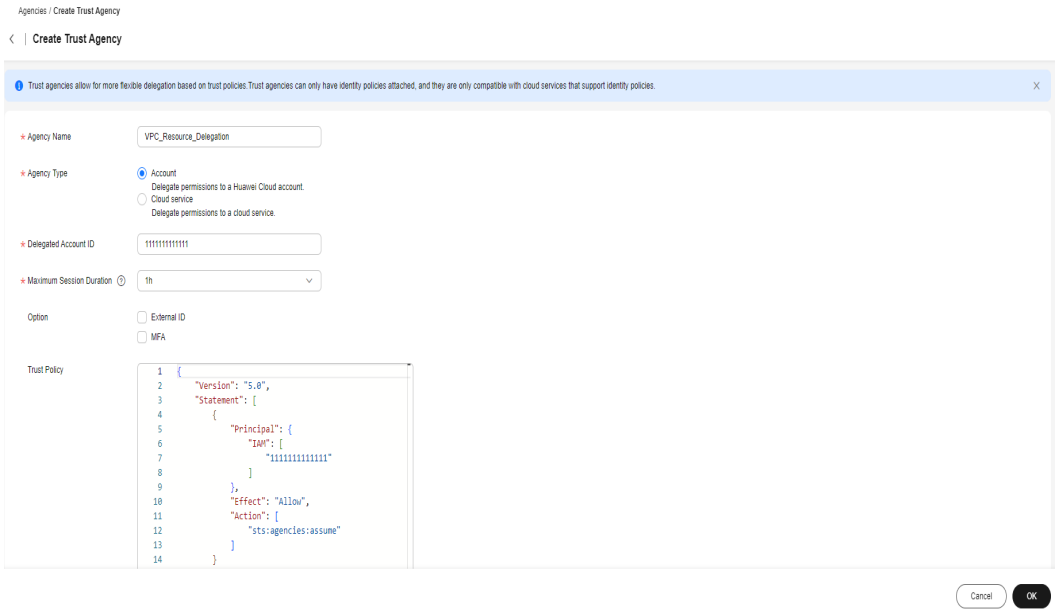
Step 1 Log in to Huawei Cloud using account A. On the IAM console, choose **Agencies** in the navigation pane.

Step 2 On the **Agencies** page, click **Create Trust Agency**. On the displayed page, set **Agency Name**, for example, **VPC_Resource_Delegation**.

Step 3 Set **Agency Type** to **Account** and enter the ID of account B in **Delegated Account ID**.

Step 4 Specify **Maximum Session Duration**

Figure 4-2 Creating a trust agency



Step 5 Choose whether to select **External ID**. The external ID of the delegated party must be unique. The external ID can be any identifier (for example, the invoice number) known only to you and the delegated party. Do not use easily-guessed information, such as the name or phone number of the delegated party. If you select **External ID**, the entered ID will be added to the trust policy for check to ensure that the delegated party performs correct operations. Note: After an external ID is used, you cannot switch the trust agency on the IAM console because the IAM console does not pass the external ID during the switch. In this case, the delegated party can use **AssumeAgency API** to pass the external ID to the target trust agency.

Step 6 Determine whether to enable MFA.

After MFA is enabled, the delegated party must enter the verification code sent to the MFA device on the login page for secondary authentication before switching the trust agency on the console.

Step 7 Edit the trust agency after it is created. The trust policy is displayed in the **Trust Policy** area.

Step 8 Enter the description and click **OK**.

Step 9 In the displayed dialog box, click **Authorize**.

Step 10 Select **VPCFullAccessPolicy** and click **OK**.

The trust agency is created and displayed in the agency list.

NOTE

If the cooperation between the two companies changes, account A can locate the target agency in the agency list and click **Modify** in the **Operation** column to modify the delegated account and permissions of the agency.

----End

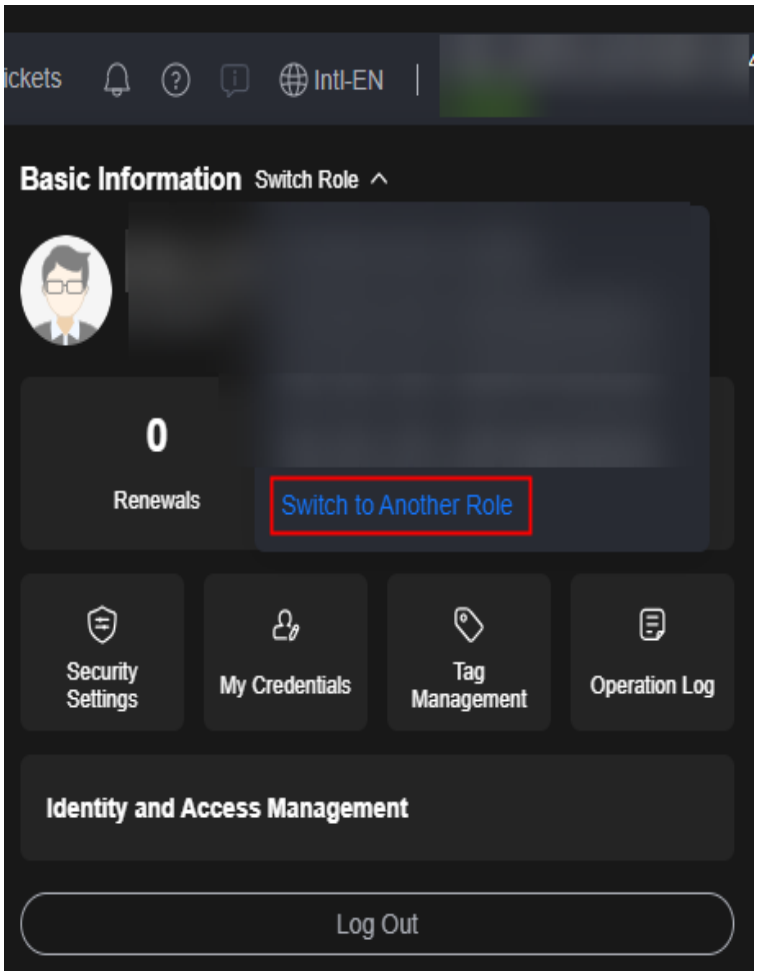
Assuming the Agency to Switch the Role (By the Delegated Party)

After the agency is created, account B (the delegated party) can assume the agency on the IAM console to switch to the account A and manage account A's resources. To do this, account B must have obtained the account name of account A and the trust agency name.

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

Step 2 Hover over the username in the upper right corner and choose **Switch Role**. You can select a role switch record or choose to switch to another role.

Figure 4-3 Switching the role

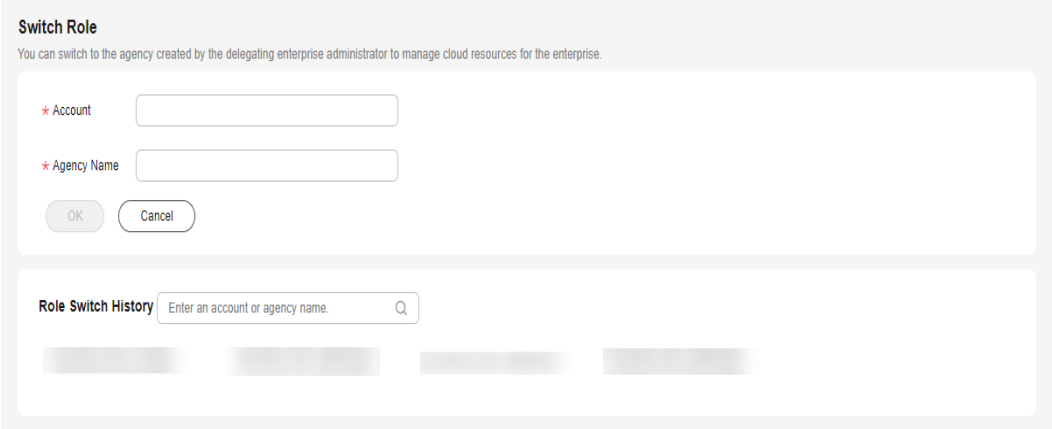


Step 3 On the displayed page, enter the account name and agency name of the delegating party. You can also click the role switch history to switch the role.

CAUTION

After entering the account name of the delegating party, only the common agencies delegated to you are listed. Trust agencies are not listed. You need to manually enter the trust agency name.

Figure 4-4 Entering the trust agency name



Step 4 Click **OK**. The account B is switched to account A and can manage VPC resources of account A.

----End

Assigning Permissions to IAM Users (by the Delegated Party)

Account B assigns trust agency's permissions to an IAM user for fine-grained authorization. Then, IAM users in account B can switch to account A to manage the resources authorized by the delegating party.

Account B must have obtained the account name of the delegating company and the agency name.

Step 1 Create a user group.

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**.

Step 2 Create custom identity policies.

1. On the **Identity Policies** page, click **Create Identity Policy**.
2. On the displayed page, enter **AssumeAgencies** for **Policy Name**.
3. Select **JSON** for **Policy View**.
4. In the **Policy Content** area, enter the following content to allow the user to manage only the trust agency with the specified ID:

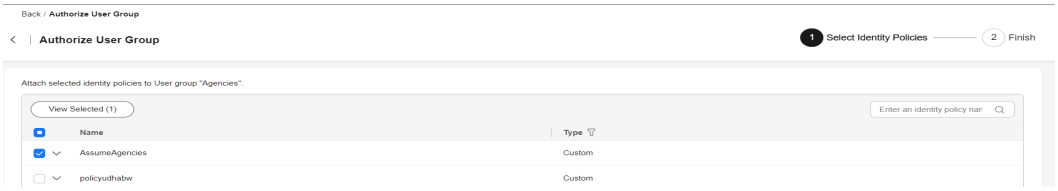
```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "sts:agencies:assume"
        ],
        "Resource": [
            "iam::<account-a-id>:agency:VPC_Resource_Delegation"
        ]
    }]
}
```


> **NOTE**
>
> Replace **<account-a-id>** with the account ID of the delegating party. You need to obtain it from the delegating party. You can copy other information without modification.

Step 3 Assign permissions to the user group.

1. Go to the user group list. The newly created user group is displayed in the list.
2. Locate this group and click **Authorize** in the **Operation** column.
3. Select the custom identity policy you created, click Next, and then click **OK**. The authorization is complete.

Figure 4-5 Authorizing a user group



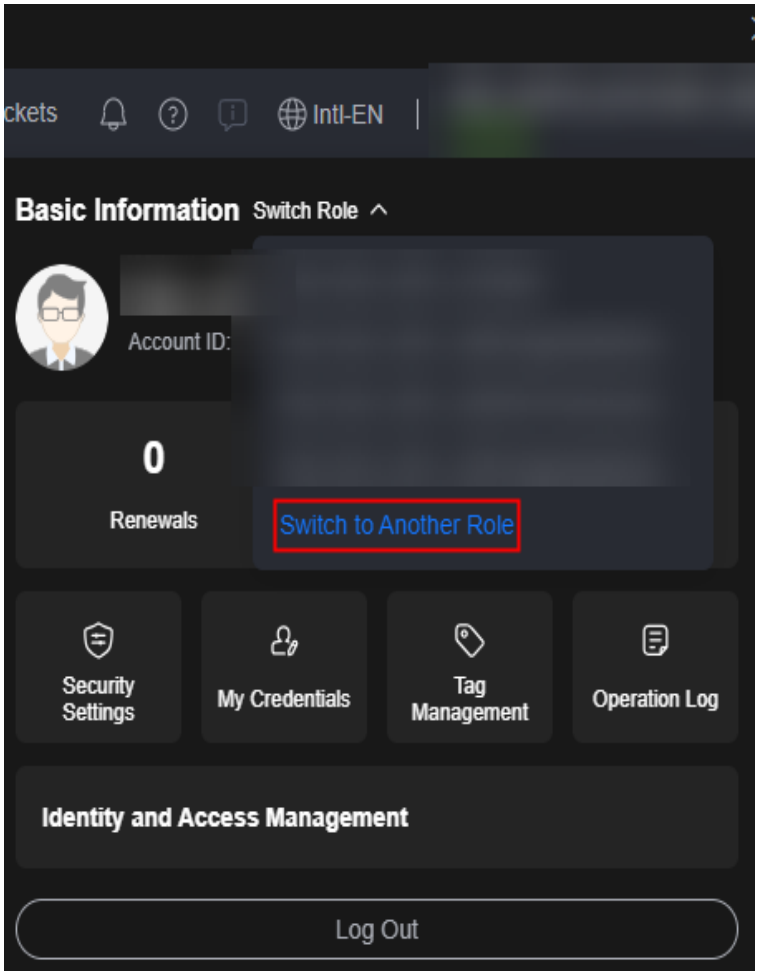
Step 4 Create a user and add it to the user group.

1. In the navigation pane, choose **Users**.
2. On the **Users** page, click **Create User**.
3. On the displayed page, enter the username and description.
4. Toggle on **Management Console Access** and select **Create an IAM User**.
5. Set **Password Setting** to **Custom**, enter a password, select **Require password reset at first login**, and click **Next**.
6. On the **Set Permissions** page, select the user group **Agency Management** created in **step 1** and click **Create User**.

Step 5 Switch the role.

1. Log in to Huawei Cloud as the IAM user created in **step 4**. For details about how to log in, see **Logging In as an IAM User**.
2. On the console, hover over the username in the upper right corner and click **Switch Role**. You can select a role from the switch record or click **Switch to Another Role**.

Figure 4-6 Switching the role



3. On the displayed page, enter the account name of the delegating party and the agency name.
4. Click **OK** to switch to the delegating account. Then, the IAM user of account B can manage resources in account A.

----End

5 Controlling Access to Resources Using Tags

Attribute-based Access Control (ABAC) is an authorization strategy that defines permissions based on attributes. Tags are a type of attributes. You can attach tags to IAM resources (including IAM users and trust agencies that can be accessed by other entities) or other Huawei Cloud resources. You can define identity policies that use tags as condition keys. This allows minimal changes to identity policies when you need to control access to a growing number of Huawei Cloud resources. ABAC policies are more flexible than role-based access control (RBAC) policies because RBAC policies require you to list each individual resource. For more information about ABAC and its advantages over RBAC, see **ABAC**.

This section describes how to create an IAM user with a principal tag, create an identity policy, and attach the policy to the IAM user. The identity policy allows the IAM user to access only the resources with the tag matching the principal tag.

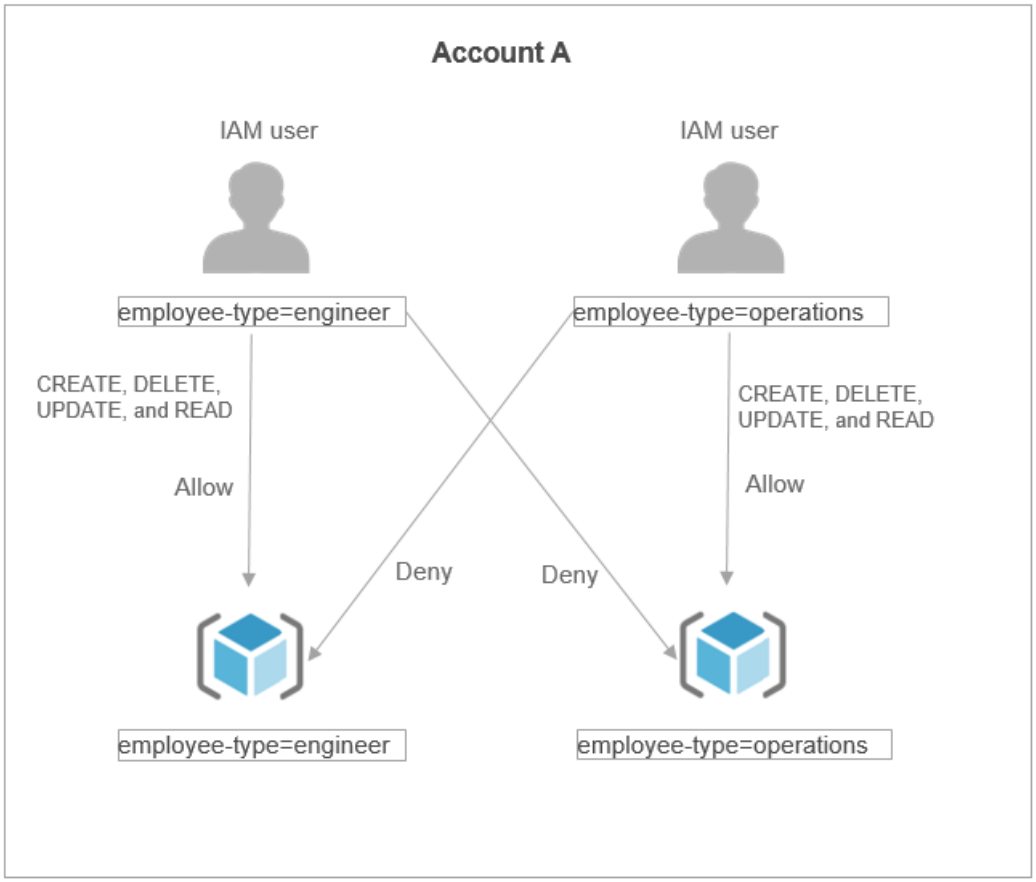
Operations

Assume that you are an experienced IAM administrator familiar with creating and managing IAM users, trust agencies, and identity policies. You want to ensure that your engineers and O&M team members can access only the resources they need. You also need an identity policy that scales as your company grows and more types of members join your company. You use principal tags and resource tags in the identity policy. For the cloud services that support resource tags, see "ABAC (Tag-based Authentication)" in **Cloud Services for Using Identity Policies and Trust Agencies**.

You can add the following tags to your engineers and O&M team members:

- employee-type=engineer
- employee-type=operations

In this section, you will tag each IAM user and each trust agency, write an identity policy, and attach the policy to the IAM user. This identity policy allows the IAM user to create, update, read, and delete accessible resources.



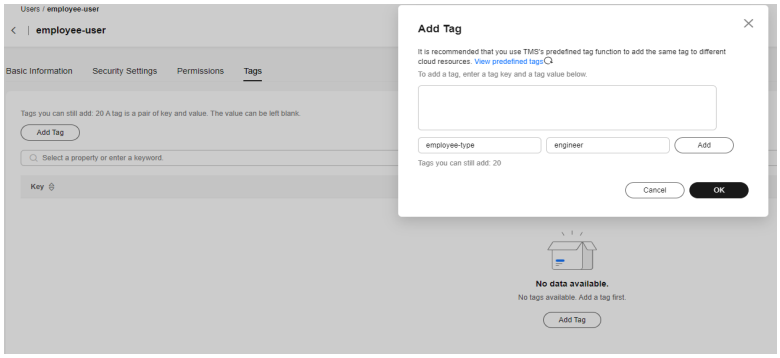
Step 1: Attach a Tag to an IAM User

Step 1 Log in to the **new IAM console** as an administrator and choose **Users** in the navigation pane.

Step 2 Click **employee-user** (the name of an IAM user for the engineer team). On the user details page, click the **Tags** tab.

Step 3 Click **Add Tag** in the upper left corner.

Step 4 In the displayed dialog box, set the tag key to **employee-type** and the tag value to **engineer**.



----End

Step 2: Attach a Tag to a Resource

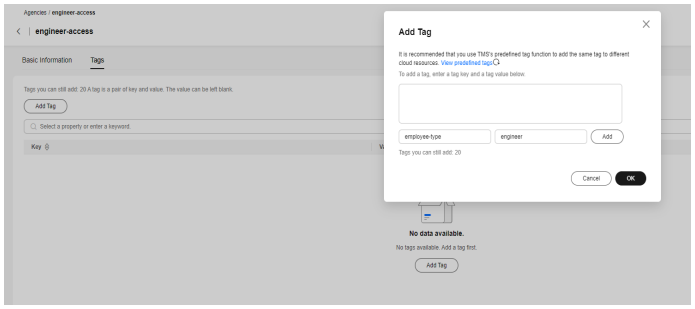
When a trust agency initiates an access, it is an IAM principal, and its tag is a principal tag. When a trust agency is accessed by an IAM principal as an IAM resource, its tag is a resource tag. The following uses trust agencies as an example:

Step 1 Log in to the **new IAM console** as an administrator and choose **Agencies** in the navigation pane.

Step 2 Click the name of the trust agency that can be accessed by the IAM user **employee-user**. On the displayed page, click the **Tags** tab.

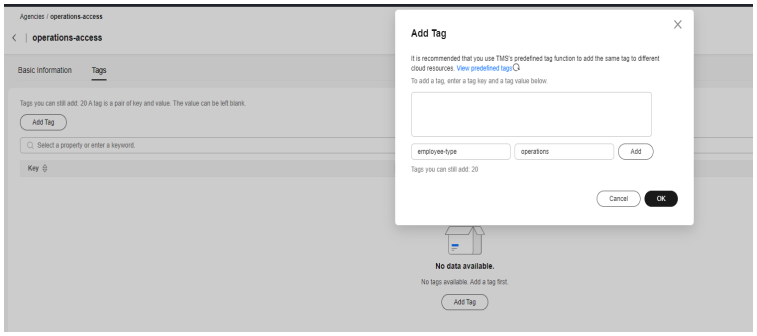
Step 3 Click **Add Tag** in the upper left corner.

Step 4 In the displayed dialog box, set the tag key to **employee-type** and the tag value to **engineer**. Click **OK**.



Step 5 Return to the trust agency list and click the name of the trust agency **operations-access** that can be accessed by the O&M team **operations**. On the displayed page, click the **Tags** tab.

Step 6 In the displayed dialog box, set the tag key to **employee-type** and the tag value to **operations**. Click **OK**.



----End

Step 3: Create a Custom Identity Policy

Step 1 Log in to the **new IAM console** as an administrator, and choose **Identity Policies** in the navigation pane.

Step 2 Click **Create Identity Policy** in the upper right corner.

Step 3 Set the identity policy name to **engineer-access-policy**.

Step 4 Set **Policy View** to **JSON**. Enter the following identity policy to allow access when the principal tag matches the tag of the resources to be accessed:

```
{
    "Version": "5.0",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "iam:agencies:getV5"
        ],
        "Condition": {
            "StringEquals": {
                "g:ResourceTag/employee-type": [
                    "${g:PrincipalTag/employee-type}"
                ]
            }
        }
    }]
}
```

Step 5 Click **OK**. The identity policy is created.

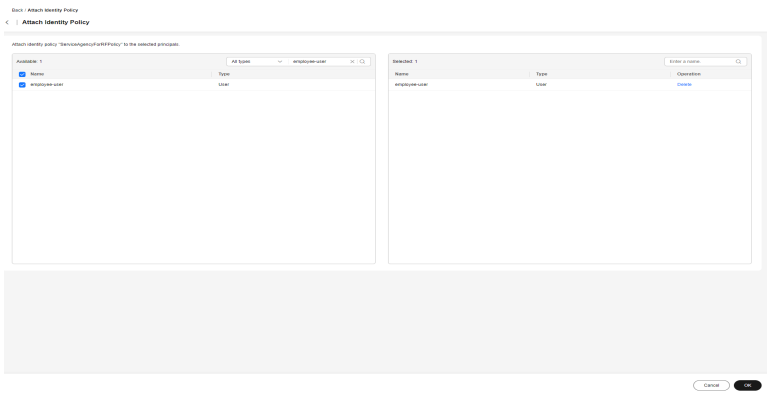
----End

Step 4: Attach the Identity Policy to the Authorization Principal

Step 1 Log in to the **new IAM console** as an administrator, and choose **Identity Policies** in the navigation pane.

Step 2 Select the identity policy created in **step 3** and click **Attach** above the identity policy list.

Step 3 Select the IAM user **employee-user** added in **step 1** and click **OK**.



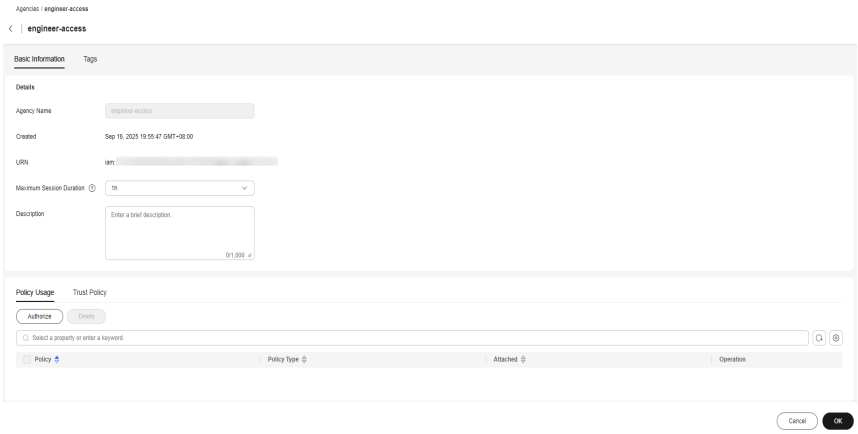
----End

Step 5: Verify the Result

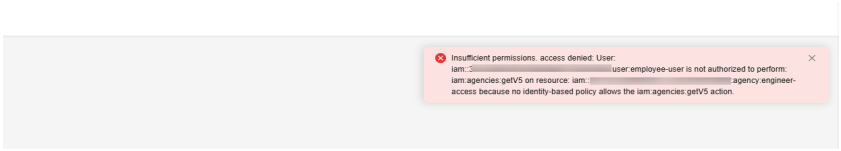
Step 1 In addition to attaching the identity policy created in **step 3** to IAM user **employee-user**, attach another identity policy that allows listing all agencies on the IAM console. (If you call APIs to list the agencies, you do not need this identity policy.)

Step 2 View the trust agencies **engineer-access** and **operations-access** as the IAM user **employee-user** of the engineer team.

- You can view the details about the trust agency **engineer-access**. This is because the principal tag of **employee-user** matches the resource tag of **engineer-access**, which complies with the identity policy.



- When you view the trust agency **operations-access**, the system displays a message indicating insufficient permissions. This is because the principal tag of **employee-user** does not match the resource tag of **operations-access**.



----End

Follow-up Operations

When new members join the company, there is no need to modify this identity policy. You only need to attach the tags to the new members and to the resources they can access.