# Contents

1 Audit

1.1 IAM Operations That Can Be Recorded by CTS

1.2 Viewing Audit Logs

2 User and User Group Management

2.1 Managing Users and Their Permissions

2.2 Managing a Project

2.3 Creating a User Group

2.4 Creating a User

2.5 Switching Projects or Regions

2.6 Viewing and Modifying User Information

2.7 Viewing and Modifying User Group Information

2.8 Changing User Permissions

3 Fine-grained Policy Management

3.1 Fine-grained Policy

3.2 Policy Language

3.3 Creating Custom Policies

4 Setting Account Security Policies

5 Agency Management

5.1 Delegating Other Accounts to Manage Resources

5.2 Creating an Agency (by a Delegating Party)

5.3 Assigning Permissions (by a Delegating Party)

5.4 Switching Roles (by a Delegated Party)

6 Federated Identity Authentication

6.1 Advantages of Federated Identity Authentication

6.2 Configuring Federated Identity Authentication

6.3 Establishing a Trust Relationship

6.4 Creating an IdP

6.5 Configuring SSO

6.6 Using Rules to Control Federated User Access to the Cloud System

6.7 Identity Conversion Rule for Federated Users

6.8 SSO Process
1.1 IAM Operations That Can Be Recorded by CTS

Table 1-1 lists IAM operations that can be recorded by CTS.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Resource Type</th>
<th>Event Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain token</td>
<td>token</td>
<td>createTokenByPwd</td>
</tr>
<tr>
<td>Obtain token</td>
<td>token</td>
<td>createTokenByHwAccessKey</td>
</tr>
<tr>
<td>Obtain token</td>
<td>token</td>
<td>createTokenByToken</td>
</tr>
<tr>
<td>Obtain token</td>
<td>token</td>
<td>createTokenByAssumeRole</td>
</tr>
<tr>
<td>Obtain token</td>
<td>token</td>
<td>createTokenByHwRenewToken</td>
</tr>
<tr>
<td>Log in</td>
<td>user</td>
<td>login</td>
</tr>
<tr>
<td>Log out</td>
<td>user</td>
<td>logout</td>
</tr>
<tr>
<td>Change user password</td>
<td>user</td>
<td>changePassword</td>
</tr>
<tr>
<td>Create user</td>
<td>user</td>
<td>createUser</td>
</tr>
<tr>
<td>Modify user information</td>
<td>user</td>
<td>updateUser</td>
</tr>
<tr>
<td>Delete user</td>
<td>user</td>
<td>deleteUser</td>
</tr>
<tr>
<td>Change user password</td>
<td>user</td>
<td>updateUserPwd</td>
</tr>
<tr>
<td>Create AK/SK</td>
<td>user</td>
<td>addCredential</td>
</tr>
<tr>
<td>Delete AK/SK</td>
<td>user</td>
<td>deleteCredential</td>
</tr>
<tr>
<td>Change email address</td>
<td>user</td>
<td>modifyUserEmail</td>
</tr>
<tr>
<td>Change mobile number</td>
<td>user</td>
<td>modifyUserMobile</td>
</tr>
<tr>
<td>Operation</td>
<td>Resource Type</td>
<td>Event Name</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Change password</td>
<td>user</td>
<td>modifyUserPassword</td>
</tr>
<tr>
<td>Enable two-factor authentication</td>
<td>user</td>
<td>modifySMVerify</td>
</tr>
<tr>
<td>Upload avatar</td>
<td>user</td>
<td>modifyUserPicture</td>
</tr>
<tr>
<td>Administrator sets user password</td>
<td>user</td>
<td>setPasswordByAdmin</td>
</tr>
<tr>
<td>Create user group</td>
<td>userGroup</td>
<td>createGroup</td>
</tr>
<tr>
<td>Update user group</td>
<td>userGroup</td>
<td>updateGroup</td>
</tr>
<tr>
<td>Delete user group</td>
<td>userGroup</td>
<td>deleteGroup</td>
</tr>
<tr>
<td>Add user to user group</td>
<td>userGroup</td>
<td>addUserToGroup</td>
</tr>
<tr>
<td>Delete user from user group</td>
<td>userGroup</td>
<td>removeUserFromGroup</td>
</tr>
<tr>
<td>Create project</td>
<td>project</td>
<td>createProject</td>
</tr>
<tr>
<td>Modify project</td>
<td>project</td>
<td>updateProject</td>
</tr>
<tr>
<td>Delete project</td>
<td>project</td>
<td>deleteProject</td>
</tr>
<tr>
<td>Update project status</td>
<td>project</td>
<td>updateProjectStatus</td>
</tr>
<tr>
<td>Cancel project deletion</td>
<td>project</td>
<td>cancelProjectDeletion</td>
</tr>
<tr>
<td>Create agency</td>
<td>agency</td>
<td>createAgency</td>
</tr>
<tr>
<td>Modify agency</td>
<td>agency</td>
<td>updateAgency</td>
</tr>
<tr>
<td>Delete agency</td>
<td>agency</td>
<td>deleteAgency</td>
</tr>
<tr>
<td>Switch role</td>
<td>user</td>
<td>switchRole</td>
</tr>
<tr>
<td>Register IdP</td>
<td>identityProvider</td>
<td>createIdentityProvider</td>
</tr>
<tr>
<td>Update IdP</td>
<td>identityProvider</td>
<td>updateIdentityProvider</td>
</tr>
<tr>
<td>Delete IdP</td>
<td>identityProvider</td>
<td>deleteIdentityProvider</td>
</tr>
<tr>
<td>Update IdP metadata</td>
<td>identityProvider</td>
<td>updateMetaConfigure</td>
</tr>
<tr>
<td>Update preset IdP metadata</td>
<td>identityProvider</td>
<td>updateSystemMetaConfigure</td>
</tr>
<tr>
<td>Register mapping</td>
<td>mapping</td>
<td>createMapping</td>
</tr>
<tr>
<td>Update mapping</td>
<td>mapping</td>
<td>updateMapping</td>
</tr>
<tr>
<td>Delete mapping</td>
<td>mapping</td>
<td>deleteMapping</td>
</tr>
<tr>
<td>Register protocol</td>
<td>protocol</td>
<td>createProtocol</td>
</tr>
<tr>
<td>Update protocol</td>
<td>protocol</td>
<td>updateProtocol</td>
</tr>
<tr>
<td>Delete protocol</td>
<td>protocol</td>
<td>deleteProtocol</td>
</tr>
<tr>
<td>Operation</td>
<td>Resource Type</td>
<td>Event Name</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Grant permissions to an agency based on account information</td>
<td>roleAgencyDomain</td>
<td>assignRoleToAgencyOnDomain</td>
</tr>
<tr>
<td>Delete permissions of an agency based on account information</td>
<td>roleAgencyDomain</td>
<td>unassignRoleToAgencyOnDomain</td>
</tr>
<tr>
<td>Grant permissions to an agency based on project information</td>
<td>roleAgencyProject</td>
<td>assignRoleToAgencyOnProject</td>
</tr>
<tr>
<td>Delete permissions of an agency based on project information</td>
<td>roleAgencyProject</td>
<td>unassignRoleToAgencyOnProject</td>
</tr>
<tr>
<td>Grant permissions to a user group under an account</td>
<td>roleGroupDomain</td>
<td>assignRoleToGroupOnDomain</td>
</tr>
<tr>
<td>Delete permissions of a user group under an account</td>
<td>roleGroupDomain</td>
<td>unassignRoleToGroupOnDomain</td>
</tr>
<tr>
<td>Grant permissions to a user group corresponding to a project</td>
<td>roleGroupProject</td>
<td>assignRoleToGroupOnProject</td>
</tr>
<tr>
<td>Delete permissions of a user group corresponding to a project</td>
<td>roleGroupProject</td>
<td>unassignRoleToGroupOnProject</td>
</tr>
<tr>
<td>Update account login policy</td>
<td>domain</td>
<td>updateSecurityPolicies</td>
</tr>
<tr>
<td>Update password policy</td>
<td>domain</td>
<td>updatePasswordPolicies</td>
</tr>
<tr>
<td>Update ACL</td>
<td>domain</td>
<td>updateACL Policies</td>
</tr>
</tbody>
</table>

### 1.2 Viewing Audit Logs

After you enable CTS, the system starts recording operations on IAM. Operation records for the last 7 days are stored on the CTS console.

**Viewing IAM Audit Logs**

1. **Step 1** Log in to the management console.
2. **Step 2** Click **Service List** in the upper part of the page and select **Cloud Trace Service** under **Management & Deployment**.
3. **Step 3** Choose **Trace List** in the navigation pane on the left.
4. **Step 4** Click **Filter** in the upper right corner of the event list to set the operation event conditions.

The following four filters are available:
Trace Source, Resource Type, and Search By
- Select the filter from the drop-down list. Select IAM for Trace Source from the drop-down list box.
- When you select Trace name for Search By, you also need to select a specific trace name.
- When you select Resource ID for Search By, you also need to select or enter a specific resource ID.
- When you select Resource name for Search By, you also need to select or enter a specific resource name.

Operator: Select a specific operator (a user rather than tenant).
Trace Status: Available options include All trace statuses, normal, warning, and incident. You can only select one of them.
You can specify start time and end time query traces during a time period.

Step 5 Click Query to view the corresponding operation event.

Step 6 Expand the details, as shown in Figure 1-1.

Figure 1-1 Expanding trace details

Step 7 Click View Trace in the Operation column. On the displayed View Trace dialog box shown in Figure 1-2, the trace structure details are displayed.

Figure 1-2 Viewing events

### View Trace

```json
{
  "service_type": "IAM",
  "user": {
    "name": "",
    "id": "d471500a6145c39b672ce6a0f3b7f9",
    "domain": {
      "name": "",
      "id": "bc264ba6ef0b4674eed1e345a"
    },
  },
  "time": "05/19/2018 09:00:06 GMT+08:00",
  "code": 302,
  "resource_type": "user",
  "resource_name": "",
  "resource_id": "6a7cc59a6145c39b672ce6a0f3b7f9",
  "source_ip": "",
  "trace_name": "login",
  "trace_type": "ConsoleAction",
  "record_time": "05/18/2018 09:00:06 GMT+08:00",
  "trace_id": "7a07f4a0-53ed-11e9-a593-260d468bc020",
  "trace_status": "normal"
}
```
2 User and User Group Management

2.1 Managing Users and Their Permissions

You can grant permissions to a user group and add users to it. Any user you add to the user group has all the permissions of the user group in the cloud system.

On the allied cloud, an Open Cloud Service Alliance user needs to create a user group with the same name as that on the hosted cloud. For details, see section Using an Allied Cloud.

**Step 1** The security administrator creates projects in a region and the projects are isolated from each other.

Figure 2-1 Project isolation model

**Step 2** The security administrator plans user groups according to users' responsibilities and grants the corresponding permissions to different user groups.
Step 3  The security administrator creates users and adds users to user groups varying by their responsibilities.

Step 4  Users can access resources in the cloud system based on their permissions.

----End
2.2 Managing a Project

Projects are used to group and isolate OpenStack resources, including computing, storage, and network resources. Resources in your account must be mounted under projects. A project can be a department or a project team. Access IAM with a security administrator to create projects in a region and perform isolated management of resources.

Procedure

**Step 1** In the navigation pane, choose **Projects**.

**Step 2** On the **Projects** page, click **Create Project**.

**Step 3** On the **Create Project** page, select a region from the **Region** drop-down list.

**Step 4** Set **Project Name**.

*NOTE*
- The project name format is Region Name_Project Name. Region Name cannot be modified.
- Only letters, digits, underscores (_), and hyphens (-) are allowed in the project name. The maximum length of Region Name_Project Name is 64 characters.

**Step 5** (Optional) Set **Description**.

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

Return to the project list. Check that **Status** of the newly created project is displayed as **Normal**.

----End

Follow-up Procedure

Authorizing projects

In the **User Group Permissions** area on the **Modify User Group** page, locate the row that contains the target project, and click **Modify**. In the displayed dialog box, select the required permission sets for the project. For details, see section **Creating a User Group**.

Related Operations

- Viewing project details
  
  a. View the projects in the corresponding region in the project list.
  
  b. Click **View** in the **Operation** column of the row that contains the target project.

  View project details and the users bound to the project.

  *NOTE*

  After the permissions on a project are granted to a user group and a user is added to the user group, the user has the permissions of the user group and is bound to the project. The user can switch projects to access different resources.

  c. Click **View** in the **Operation** column in the user permission list.

  View the permissions of the users bound to the project.
### 2.3 Creating a User Group

You can plan user groups based on users' responsibilities and grant them the corresponding permissions. Users in a user group have all of its permissions. User groups help improve the efficiency of permission management.

#### Default User Group

Table 2-1 describes the default user groups and their permissions provided by IAM.

- For an existing account, IAM provides default user groups **admin** and **power_user**.
- For a newly registered account, IAM provides only the default user group **admin**.

<table>
<thead>
<tr>
<th>User Group Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>This user group has all operation permissions for all cloud service resources. A user in this group can operate and use all cloud service resources, including but not limited to creating user groups and users, modifying user group permissions, and managing OBS resources.</td>
</tr>
<tr>
<td>power_user</td>
<td>This group has all operation permissions except user management. A user in this group can manage all cloud service resources. However, the user cannot create user groups or users, modify user group permissions, or grant permissions to users.</td>
</tr>
</tbody>
</table>

#### Procedure

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

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

**Step 3** Enter a user group name.

**Step 4** (Optional) Set **Description**.

**Step 5** Click **OK**.

The user group list is displayed, including the newly created user group.
Step 6 Click Modify in the Operation column of the row that contains the newly created user group.

Step 7 Click Configure Permission in the Operation column of the row that contains the newly created user group.

Step 8 In the User Group Permissions area, click Modify in the Operation column of the row that contains the target project.

**Note**
The permissions granted to the user group only take effect for the current project. If you need to grant the permissions for multiple projects to the user group, you must grant permissions for each project individually by clicking Modify in the row that contains the corresponding project.

Step 9 Configure policies for the user group.

**Note**
You can enter a keyword to quickly find the target policy.

Step 10 Click OK.

----End

### 2.4 Creating a User

To share the resources in your account with other users, access IAM as a security administrator to create users and specify security credentials and permissions for them. These users can access the cloud system using the management console or a development tool (such as APIs, the CLI, and SDK).

**Procedure**

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

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

**Step 3** On the Create User page, enter Username.

**Step 4** Specify Credential Type.

<table>
<thead>
<tr>
<th>Credential Type</th>
<th>Application Scenario</th>
</tr>
</thead>
</table>
| Password        | • Used to log in to the management console  
|                 | • Used to enable development tools (such as APIs, the CLI, and SDK) that can access cloud services through password authentication |
| Access Key      | Used to enable development tools (such as APIs, the CLI, and SDK) that can access cloud services through key authentication |

**Step 5** Select a user group which you want to add the user from the drop-down list box in the User Groups area.

**Note**

• You can also enter a keyword to quickly find the target user group.

• A user can be added to multiple user groups.
Perform one of the following based on the credential type you selected in Step 4.

<table>
<thead>
<tr>
<th>Credential Type</th>
<th>Follow-up Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Go to Step 6.</td>
</tr>
<tr>
<td>Access Key</td>
<td>Click OK. Download the generated key. User creation is complete. <strong>NOTE</strong> Access keys are credentials for identity authentication in IAM. You can only obtain an access key by downloading it. If the user needs to use an access key for authentication in IAM but it has not been downloaded, you must generate a new access key.</td>
</tr>
</tbody>
</table>

**Step 6** Click Next.

**Step 7** Specify **Password Type**.

<table>
<thead>
<tr>
<th>Password Type</th>
<th>Description</th>
<th>Follow-up Procedure</th>
</tr>
</thead>
</table>
| Set at first login| The system will send you a one-time login link through email. You need to use this link to set a password before you can log in to the management console. | 1. Set Email for receiving the login link.  
2. (Optional) Set Mobile Number.  
3. Click OK. |
| Automatically generated | The system randomly generates a 10-character password. This option enables development tools (such as APIs, the CLI, and SDK) that can access cloud services through password authentication. | 1. (Optional) Set Email.  
2. (Optional) Set Mobile Number.  
3. Click OK.  
4. Download the password file. |
<table>
<thead>
<tr>
<th>Password Type</th>
<th>Description</th>
<th>Follow-up Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set manually</td>
<td>Users set their own passwords.</td>
<td>1. (Optional) Set Email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. (Optional) Set Mobile Number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The password must meet the following requirements:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- It must be 6 to 32 characters long.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- It must contain at least 2 of the following</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- uppercases letters, lowercase letters, digits,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- and special characters ('&quot;#$%&amp;'()*+,-./:;&lt;=&gt;?@ [ ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- can include spaces).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- It cannot be the username or the username</td>
</tr>
<tr>
<td></td>
<td></td>
<td>spelled backwards. For example, if the username is</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A12345, the password cannot be A12345,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a12345, 54321A or 54321a.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- It cannot contain the user's mobile number or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>email address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Click OK.</td>
</tr>
</tbody>
</table>

**NOTE**
- The SMS-based login verification function can be enabled only when a user is bound with an email address and a mobile number.
- You can log in to the system with your username, mobile number, or email address.
- If you forget your password, you can reset it using the email address or mobile number that was bound to your account.

**Step 8** If you select *Automatically generated* or *Set manually*, choose whether to require password reset at the next login. This function is enabled by default to ensure account security.

**Step 9** Click **OK**.

The user is created successfully.

----End

**Related Operations**
- View and modify information about the user, including the user status, bound email address, bound mobile number, user group, and logs.
- Delete a user. In the user list, click **Delete** in the row that contains the target user.

**2.5 Switching Projects or Regions**

Resources in different projects or regions are isolated. You can only access the resources in authorized projects or regions. If you do not have permissions for the current project or region, you must first switch to an authorized project or region.
Procedure

Step 1 At the upper left of the main menu bar, click Console.

Step 2 In the upper left corner, select the project or region to be accessed from the drop-down list. After you have switched to the target project or region successfully, you can access its resources.

----End

2.6 Viewing and Modifying User Information

Administrators can view and modify the basic information of a user, belonged user groups, and logs generated for the user. They can change the group of a user after the user's responsibilities change, or modify the login credentials of a user if the user's API password or access key was forgotten or lost.

Viewing User Information

In the user list, click next to a user to view the detailed user information, including Basic Information, User Groups, and User Logs.

Modifying User Information

Click Modify in the Operation column of the row that contains the target user.
Status: A user is enabled by default after being created. You can change the status of a user to Disabled if you do not use it again.

Login authentication method
- Virtual MFA: Change the login authentication mode of a user to virtual MFA only if the user has been bound to an MFA device. After the change, the user must enter virtual MFA verification codes when logging in.
- SMS: Change the login authentication mode of a user to SMS only if the user has been bound to a mobile number. After the change, the user must enter a mobile verification code when logging in.
- Email: Change the login authentication mode of a user to SMS only if the user has been bound to an email address. After the change, the user must enter an email verification code when logging in.
- Custom: You can set another login authentication mode on the My Credentials page.
- Disable: Disable login authentication. Secondary authentication is not required when the user logs in.

Email, Mobile Number, and Description

Virtual MFA Device: Bind an MFA device to or unbind an MFA device from a user.
User Groups: Add a user to or remove it from target user groups.

**NOTE**
Enter a keyword to quickly find the target user group.

Setting User Credentials

In the user list, click Set Credentials in the Operation column of the row that contains the target user to change its API password or manage its access keys.

<table>
<thead>
<tr>
<th>Credential Type</th>
<th>Generation Method</th>
<th>Description</th>
<th>Application Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Using email</td>
<td>The system will send you a one-time login link through email. You can click this link to log in to the management console and set the password.</td>
<td>Used to reset the API passwords of users who have email addresses bound to their accounts. The user needs to use the password to log in to the management console.</td>
</tr>
<tr>
<td></td>
<td>Automatically generated</td>
<td>The system randomly generates a 10-character API password. <strong>NOTE</strong> Click OK to download the automatically generated password file.</td>
<td>Used to reset the password of a user who is using a development tool (such as APIs, the CLI, and SDK) that can access the cloud system through password authentication.</td>
</tr>
<tr>
<td></td>
<td>Set manually</td>
<td>Users set their own API passwords.</td>
<td>Used to reset any user's API password.</td>
</tr>
<tr>
<td>Access key</td>
<td>Created by a user or a security administrator</td>
<td>Users can add or delete access keys in the Access Keys area. <strong>NOTE</strong> Each user can create a maximum of two access keys, which are valid within 360 days. To ensure account security, keep them securely.</td>
<td>Users can access the cloud system by using access keys.</td>
</tr>
</tbody>
</table>

- **Require Password Reset**: If you select Automatically generated or Set manually, you can choose whether to require password reset at the next login. This function is enabled by default to ensure account security.
- **Resetting the failed login count**
  In the user list, click Reset Failed Logins in the Operation column of the row that contains the target user to reset the failed login count of the user and unlock the user.
2.7 Viewing and Modifying User Group Information

Security administrators can view and modify a user group’s basic information, permissions, and users. You can change users’ permissions by changing their group.

Procedure

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

**Step 2**  In the user group list, view or modify user group information.

- **Viewing user group information**
  In the user group list, view user group details. The detailed information includes **Basic Information**, **User Group Permissions**, and **Group Members**.

- **Modifying user group information**
  Click **Modify** in the **Operation** column of the row that contains the target user group to go to the **Modify User Group** page.

**NOTE**
- You can modify users in the default user groups but you cannot modify the basic information or permissions of those user groups.
- A user group is a credential associated with federated authentication and its name cannot be changed.

<table>
<thead>
<tr>
<th>Information to Be Modified</th>
<th>Method</th>
</tr>
</thead>
</table>
| User group permissions     | 1. Click **Modify** in the **Operation** column of the row that contains the project to be authorized for the user group.  
2. On the displayed **Modify Policy** page, select required policies.  
3. Click **OK**. |
| Users in the user group    | - Adding a user  
In the **Group Members** area, select a user to be added from the drop-down list.  
**NOTE**  
You can enter a keyword to quickly find the target user.  
- Deleting a user  
In the **Group Members** area, delete a user from the user group. |

**Step 3**  In the user group list, you can perform the following operations:

- **Viewing user group information**

  In the user group list, click to view user group details. The detailed information includes **Basic Information**, **User Group Permissions**, and **Group Members**.
Modifying user group description
In the user group list, click Edit to modify the description of the user group.

Managing a user
In the user group list, click Manage User.
- Adding a user to a user group
  Select the user to be added from the Available Users list.
  **NOTE**
  - If there are no available users, create one first.
  - You can enter a keyword to quickly find the target user.
- Deleting a user from a user group
  In the Selected Users area, delete a user from the user group.

Configuring permissions
In the user group list, click Configure Permission to modify the permissions of the user group.

a. Click Configure Policy in the Operation column of the row that contains the target project.
  i. Select the policy to be added from the Available Policies list.
  ii. Delete the target policy from the Selected Policies list.
b. Click OK.

Deleting a user group
In the user group list, click Delete in the Operation column that contains the unnecessary user group.

2.8 Changing User Permissions

You can use the following methods to change user permissions:

- Change the user group of a user on the Modify User page. This method is used when the permissions of a single user have changed. For details, see Viewing and Modifying User Information.
- Change the permissions of a user group or change the users included in the user group. This method is used when adding or deleting multiple users from a user group. For details, see Viewing and Modifying User Group Information.
3 Fine-grained Policy Management

3.1 Fine-grained Policy

A fine-grained policy is a set of permissions defining which operations on which cloud services can be performed. Each policy can define multiple permission sets. After a policy is granted to a user group, users in the user group obtain the permissions of the policy. IAM implements fine-grained permission management based on the permissions defined by policies.

IAM supports two types of policies:

- **Default policies**: define the common permissions preset in the system, which are typically read-only or management permission for different cloud services such as ECS. Default policies can be used only for authorization and cannot be edited or modified.
- **Custom policies**: define the permissions created and managed by users and are the extension and supplement of default policies.

3.2 Policy Language

Policy Content

A fine-grained authorization policy consists of the policy version (the **Version** field) and authorization statement (the **Statement** field).

- **Version**: Used to identify role-based access control (RBAC) policies and fine-grained policies.
  - **1.0**: RBAC policies, which are preset in the system and used to grant permissions of each service as a whole. After such a policy is granted to a user, the user has all permissions of the corresponding service.
  - **1.1**: Fine-grained policies, which enable more refined authorization based on service APIs. After such a policy is granted to a user, the user can only perform specific operations on the corresponding service. Fine-grained policies are classified into default and custom policies.
    - **Default policies**: Preset common permission sets to control read and administrator permissions of different services.
Custom policies: Permission sets created and managed by users as an extension and supplement of default policies. For example: A custom policy can be created to allow users only to modify ECS specifications.

- **Statement**: Detailed information about a policy, containing the **Effect** and **Action** elements.
  - **Effect**:
    Valid values for Effect include Allow and Deny. In a custom policy that contains both Allow and Deny statements, the Deny statements take the precedence.
  - **Action**:
    The value can be one or more resource authorization items. The value format is `Service name:Resource type:Action`, for example, `vpc:ports:create`.

**NOTE**
- **Service name**: indicates the product name, such as `ecs`, `evs`, or `vpc`. Only lowercase letters are allowed.
- **Resource type and Action**: The values are case-insensitive, and the wildcard (*) are allowed. A wildcard (*) can represent all or part of information about resource types and actions for the specific service.

**Example Policies**

- A policy can define a single permission, such as the permission to query ECS details.
  ```json
  { 
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:servers:list",
        "ecs:servers:get",
        "ecs:serverVolumes:use",
        "ecs:diskConfigs:use",
        "ecs:securityGroups:use",
        "ecs:serverKeypairs:get",
        "vpc:securityGroups:list",
        "vpc:securityGroups:get",
        "vpc:securityGroupRules:get",
        "vpc:networks:get",
        "vpc:subnets:get",
        "vpc:ports:get",
        "vpc:routers:get"
      ]
    }
  ]
  }
  ```

- A policy can define multiple permissions, such as the permissions to lock ECSs and create EVS disks.
  ```json
  { 
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:servers:lock",
        "evs:volumes:create"
      ]
    }
  ]
  }
  ```
The following example shows how to use the wildcard (*) to define all permissions on Image Management Service (IMS) resources.

```json
{
   "Version": "1.1",
   "Statement": [

      {
         "Action": [
            "ims:*:*",
            "ecs:*:list",
            "ecs:*:get",
            "evs:*:get"
         ],
         "Effect": "Allow"
      }
   ]
}
```

## Authentication Logic

IAM authenticates users according to the permissions that have been granted to them. The authentication logic is as follows:

**Figure 3-1 Authentication logic**

- **Access request**
- **System authentication**
- **Is there any explicit deny?**
  - Yes: Final decision: Deny
  - No: **Is there any explicit allow?**
    - Yes: Final decision: Allow
    - No: Final decision: Deny

**NOTE**

The actions in each policy bear the OR relationship.
1. A user accesses the system and initiates an operation request.
2. IAM evaluates all the access policies that have been granted to the user.
3. In these policies, IAM looks for explicit deny instructions. If IAM finds an explicit deny that applies, it returns a decision of Deny, and the authentication ends.
4. If no explicit deny is found, IAM looks for Allow instructions that would apply to the request. If IAM finds an explicit permit that applies, it returns a decision of Allow, and the authentication ends.
5. If no explicit permit is found, IAM returns a decision of Deny, and the authentication ends.

3.3 Creating Custom Policies

If the default policies cannot meet the requirements on fine-grained access control, you can create custom policies and assign the policies to the user group.

Procedure

Step 1 In the navigation pane, choose Policies.
Step 2 On the Policies page, click Create Custom Policy.
Step 3 Enter Policy Name.
Step 4 Set Scope.
Specify the scope in which the custom policy will take effect. Cloud services are classified into global-level and project-level services based on the locations they are deployed.

- **Global-level service**: Deployed globally without differentiating physical areas. When creating custom policies for globally deployed services, specify the scope as **Global-level service**. Custom policies of this scope must be granted to user groups in the Global project.

- **Project-level service**: Deployed in one or more regions. When creating custom policies for regionally deployed services, specify the scope as **Project-level service**. Custom policies of this scope must be granted to user groups in the project or subproject corresponding to the deployment region.

For example, when creating a fine-grained policy ("evs:volumes:create") for Elastic Volume Service (EVS), which is a project-level service, set Scope to **Project-level service**. If the policy will take effect for multiple projects, authorization is required for each of the projects.

Step 5 (Optional) Enter Description.

Step 6 In the Policy Information area, click Select Template. For example, select VPC Admin as the template.

Step 7 Click OK.

Step 8 Modify Effect and Action values in the Statement field in the template. For details, see section **Policy Language**.

- **Effect**: The value can be Allow and Deny. If both Allow and Deny are found in statements, the policy evaluation starts with Deny.
**Action**: Fill the **Action** field with the permissions in the API permissions table (see Figure 3-2) of the specific service, for example, `evs:volumes:create`. IAM then implements fine-grained authorization by calling the corresponding APIs in the table.

**Figure 3-2 API permissions**

<table>
<thead>
<tr>
<th>API</th>
<th>API Function</th>
<th>Permissions</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST /v2/project_id/cloudvolumes</td>
<td>Create EVS disks.</td>
<td>evs:volumes:create</td>
<td>- Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Enterprise project</td>
</tr>
</tbody>
</table>

**NOTE**
- The **Version** value of a custom policy must be 1.1.
- A custom policy can contain statements of multiple services that are all global or project-based.
- Policies support only API-level authorization. You need to fill the **Action** field with the permissions in the API permissions table of the specific service. IAM then implements fine-grained authorization by calling the corresponding APIs in the table. If the scope of all permissions in a custom policy includes **Project** and **Enterprise Project**, the custom policy can be granted on both IAM and Enterprise Management. If the scope of all permissions includes only **Project**, the custom policy can be granted and takes effect only on IAM.

**Step 9** Click **OK**.

**NOTE**
If a message is displayed indicating that the syntax is incorrect, modify policy information according to the policy syntax.

The custom policy is created successfully. You can select a custom policy from the user group to implement fine-grained authorization.

-----End

**Follow-up Operation**

- **Modifying custom policies**
  You can modify custom policies if user permissions have changed.
  On the **Policies** page, click **Modify** in the **Operation** column of the target policy, and modify the name, description, and policy information.

- **Deleting custom policies**
  You can delete custom policies if they are no longer needed.
  On the **Policies** page, click **Delete** in the **Operation** column of the target policy to delete it.

- **Attaching a custom policy to a user group (The users in the group have all the permissions defined by the policy.)**
  a. Click **Modify** in the **Operation** column of the row that contains the target user group.
  b. In the **User Group Permissions** area, click **Modify** in the **Operation** column of the row that contains the target project.
c. In the **Available Policies** area on the **Modify Policy** page, select a newly created custom policy.
Users with the **Security Administrator** permission can set a login authentication policy, API password policy, ACL, and operation security protection to improve user information and system security.

**Procedure**

**Step 1** Set login verification policies.

1. In the navigation pane, choose **Account Settings > Login Authentication Policies**.

2. In the **Account Locking Policy** area, enter **Duration**, **Maximum Number of Attempts**, and **Locking Duration**.
   
   If the number of login attempts reaches the specified upper limit within the specified duration, the user account will be locked for a period of time. For example, if a user fails to log in for three consecutive times within 10 minutes, the user account will be locked for 15 minutes. The user can try again in 15 minutes.

3. In the **Account Locking Policy** area, enter **Duration** and **Maximum Number of Attempts**. If the number of login attempts reaches the specified upper limit within the specified duration, the user account will be locked and can be unlocked only by the security administrator.

4. In the **Account Disabling Policy** area, select **If an account is not used within the validity period, it will be disabled**. Then set **Account Expiration**. If the user does not access the cloud system through the management console or API within the set **Account Expiration**, the account will be disabled.

   **Account Disabling Policy** is set to protect the account. After the account is disabled, resources in the account are not affected. You can contact the administrator to enable the account again.

5. In the **Session Timeout Policy** area, set **Session Timeout Duration**. The default value is 15 minutes. You can set the session timeout duration from 15 minutes to 24 hours. If the user does not perform any operation within the specified duration, the user needs to log in again.

6. In the **Session Timeout Policy** area, set **Session Timeout Duration**. The default value is 60 minutes. You can set the session timeout duration from 15 minutes to 24 hours. If the user does not perform any operation within the specified duration, the user needs to log in again.

7. In the **Recent Login Information** area, select **Display last login information upon a successful login**.
Users can view login information, such as the time of their last login, on the Login Verification page.

8. In the Login Verification Information area, customize the verification information, which is displayed upon a successful login.

Users can view this customized information on the Login Verification page.

9. Click OK.

**Step 2** Set password policies.

1. In the navigation pane, choose Account Settings > Password Policies.
2. In the Setting Policy area, set the parameters as follows:
   - Set Minimum Number of Characters.
     
     **NOTE**
     
     The default value of Minimum Number of Characters is 6.
   - Select Disallow same consecutive characters in a password and set Maximum Number of Same Consecutive Characters.
   - Select Disallow password repetition and set Most Recent Passwords Disallowed.
3. In the Expiration Policy area, select Force password change upon password expiration (You are prompted to change your password 15 days before password expiration). Then set Password Validity Period.

   This setting only allows a user with an expired password to log in to the system after the user has changed their password.

   **NOTE**
   
   The password must meet the following requirements:
   - It must be 6 to 32 characters long.
   - It must contain at least 2 of the following character types: uppercase letters, lowercase letters, digits, and special characters ("#$%&'()*+,-./:;<=>?@\]^`{|}~ and spaces).
   - It cannot be the username or the username spelled backwards. For example, if the username is A12345, the password cannot be A12345, a12345, 54321A or 54321a.
   - It cannot contain the user's mobile number or email address.
4. In the Minimum Password Validity Period Policy area, select A new password can be changed only after it has been used for the specified minimum password validity period and set Minimum Password Validity Period.

   After the password has been changed, you can only change it again after the time specified by Minimum Password Validity Period has elapsed.

5. Click Apply.

**Step 3** Set API password policies.

1. In the navigation pane, choose Account Settings > API Password Policies.
2. In the Setting Policy area, set the parameters as follows:
   - Set Minimum Number of Characters.
     
     **NOTE**
     
     The default value of Minimum Number of Characters is 6.
   - Select Disallow same consecutive characters in an API password and set Maximum Number of Same Consecutive Characters.
   - Select Disallow API password repetition and set Most Recent API Passwords Disallowed.
3. In the **Expiration Policy** area, select **Force API password change upon API password expiration** (You are prompted to change your API password 15 days before API password expiration). Then set **API Password Validity Period**.  
This setting only allows a user with an expired API password to log in to the system after the user has changed their password.

**NOTE**
An API password must meet the following requirements:
- It must be 6 to 32 characters long.
- It must contain at least 2 of the following character types: uppercase letters, lowercase letters, digits, and special characters ("#%&()+,-./:;<=>?@[\]^`{|}~ and spaces).
- It cannot be the username or the username spelled backwards. For example, if the username is A12345, the password cannot be A12345, a12345, 54321A or 54321a.
- It cannot contain the user's mobile number or email address.

4. In the **Minimum Password Validity Period Policy** area, select **A new password can be changed only after it has been used for the specified minimum password validity period** and set **Minimum Password Validity Period**.  
After the API password is changed, you can only change it again after the time specified by **Minimum API Password Validity Period** has elapsed.

5. Click **Apply**.

**Step 4** Set an ACL.

1. In the navigation pane, choose **Account Settings > ACLs**.

**NOTE**
ACL validation conditions:
- Accessing cloud services by using the management console: An ACL takes effect for the users in the account but not for the account itself.
- Accessing cloud services by calling APIs: An ACL takes effect for the account itself and the users in the account. When an ACL is modified, it takes effect two hours later.

2. On the **ACLs** page, enter the allowed IP addresses or network segments.
   - **Allowed IP Address Range**: only allows users to access the system using specified IP addresses.
   - **Allowed IP Addresses or Network Segments**: only allows users to access the system using specified IP addresses or network segments.

   For example: 10.10.10.10/32.

**NOTE**
- You can click **Restore Defaults** to restore the allowed IP address range to the default value, 0.0.0.0-255.255.255.255, and to clear **Allowed IP Addresses or Network Segments**.
- If both **Allowed IP Address Range** and **Allowed IP Addresses or Network Segments** are set, users are allowed to access the system if their IP address meets the conditions specified by either of the two parameters.

3. Click **Apply**.

**Step 5** Set operation security protection. If this function is enabled, authentication is required for high-risk operations. For example, a user needs to enter the verification code when deleting an access key.

1. In the navigation pane, choose **Account Settings > Operation Security**.
2. Enable operation security protection.
NOTE

- Operation security protection is disabled by default.
- High-risk operations are defined by each service.
- When a user performs a high-risk operation, the Operation Security page is displayed. Select a verification mode, email verification or phone verification.
  - If users have bound only mobile numbers to their accounts, only phone verification can be selected.
  - If users have bound only email addresses to their accounts, only email verification can be selected.
  - If users have bound both mobile numbers and email addresses to their accounts, phone verification is selected by default. Users can manually change the verification mode to email verification.
  - If users have not bound mobile numbers or email addresses to their accounts, operation security verification does not take effect. The operation is allowed by default.

----End
5 Agency Management

5.1 Delegating Other Accounts to Manage Resources

You can grant your operation permissions to more professional, efficient accounts or cloud services to manage your resources.

This section uses account A and account B as an example to describe how to delegate another account to manage resources under an account.

Step 1  Account A creates an agency.

Figure 5-1 Agency creation model

Step 2  Account B grants user B permissions for managing account A's resources.

1. Create a user group (for example, Agency), and grant resource management permissions to the user group.
2. Add user Job to user group **Agency**.

**Figure 5-2** Permission granting model

![Permission granting model](image)

**Step 3** User Job of account B manages the resources in account A.
1. Job logs in to the cloud system and switches the role to account A.
2. Job switches to project A.
3. Job manages the resources in account A based on permissions.

**Figure 5-3** Agency management model

![Agency management model](image)

---End

5.2 Creating an Agency (by a Delegating Party)

By creating an agency, you can share your resources with other accounts, or delegate more professional personnel or teams to manage your resources. The delegated account can log in to the cloud system and switch to your account to manage your resources. You do not need to share security credentials (such as passwords and access keys) with other accounts, ensuring the security of your account.

**Procedure**

**Step 1** In the navigation pane, choose **Agencies**.

**Step 2** On the **Agencies** page, click **Create Agency**.

**Step 3** Specify **Agency Name** and **Agency Type**.
### Table 5-1 Agency types

<table>
<thead>
<tr>
<th>Agency Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common account</td>
<td>Common accounts in the cloud system. This agency type is used to share resources with other accounts or delegate other accounts to manage the resources in your account.</td>
</tr>
<tr>
<td>Cloud service</td>
<td>Services in the cloud system. This agency type is used to authorize cloud services to access or maintain user data. For example, after an agency with ECS is created, ECS can obtain users’ access keys to call APIs, facilitating O&amp;M and monitoring.</td>
</tr>
</tbody>
</table>

**NOTE**  
After you create an agency with **Agency Type** set to **Cloud service**, the agency cannot be modified.

- If you set **Agency Type** to **Common account**, enter the domain name of a common account for which the trust relationship is to be established in **Delegated Account**.
- If you set **Agency Type** to **Cloud service**, click **Select** and set the cloud service.

**Step 4**  
Set **Validity Period** and enter **Description**.

**Step 5**  
In the **Permissions** area, locate the row that contains the target region and project and click **Modify** in the **Operation** column, and select policies for the delegating enterprise.

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

The newly created agency is displayed in the agency list. The delegated account can manage resources in the delegating account by switching the role.

---End

**Follow-up Operation**

In the agency list, you can click **Modify** in the row that contains the newly created agency to modify the basic information about the agency, such as the permissions and validity period of the agency.

**NOTE**  
You can only modify an agency whose **Agency Type** is set to **Common account**.

### 5.3 Assigning Permissions (by a Delegated Party)

When an account establishes a trust relationship between itself and your account, you become a delegated party. You can authorize a user to manage resources of the delegating party. After an account establishes multiple trust relationships between itself and your account, you can authorize different users to manage resources of the delegating party. However, each user can switch to only the delegated agencies. You can create custom policies to grant specified permissions to users.
Prerequisites

- An account has created the trust relationship with you.
- You have obtained the name of the delegating account and the name and ID of the created agency.

Procedure

Step 1  Create a custom policy.

NOTE
- To delegate a specific agency to a user, perform the following steps.
- To delegate all agencies to a user, go to Step 2.

1. In the navigation pane, choose Policies.
2. On the Policies page, click Create Custom Policy.
3. Enter a policy name.
5. In the Policy Information area, enter the following content:

```json
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": ["iam:agencies:assume"],
         "Resource": {
            "uri": ["/iam/agencies/b36b1258b5dc41a4aa8255508xxx..."],
            "url": ["/iam/agencies/b36b1258b5dc41a4aa8255508xxx..."
         ],
         "Effect": "Allow"
      }
   ]
}
```

NOTE
- Copy and paste all the content, and replace b36b1258b5dc41a4aa8255508xxx... with the ID of the agency to be granted.
- This procedure provides only required operations for fine-grained authorization. For more information about fine-grained policies, see Fine-grained Policy Management.

6. Click OK.

Step 2  Create a user group and grant permissions to it.

1. In the navigation pane, choose User Groups.
3. Enter a user group name.
4. Click OK.

The user group list is displayed, including the newly created user group.

5. Click Modify in the Operation column of the row that contains the newly created user group.
6. Click Configure Permission in the Operation column of the row that contains the newly created user group.
7. In the **User Group Permissions** area, click **Modify** in the **Operation** column of the row that contains the **Global** project.

8. On the **User Group Permissions** tab page, click **Configure Policy** in the **Operation** column of the row that contains the **Global** project.

9. Select the policy created in **Step 1** or the **Agent Operator** permission.

   **NOTE**
   - Custom policy: Allows a user to access only a specified agency.
   - **Agent Operator** permission: Allows a user to access all agencies.

10. Click **OK**.

#### Step 3 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 **Create User** page, enter a username.
4. Select **Password** for **Credential Type**.
5. Select the user group created in **Step 2** from the drop-down list box in the **User Groups** area.
6. Click **Next**.
7. Select **Set at first login** for **Password Type**.
8. Enter an email address.
9. Click **OK**.

#### Step 4 Switch your roles.

1. Log in to the system as the user created in **Step 3**.
2. Click the logged-in account in the upper right corner of the page and choose **Switch Role**.
3. On the **Switch Role** page, enter the name of the delegating account.

   **NOTE**
   The system automatically matches the account to an agency. If the matched agency has not been delegated, you have no permissions to access the account. However, you can remove the agency and select an authorized one from the drop-down list box.

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

----End

**Follow-up Operation**

Click the delegating account in the upper right corner of the page and choose **Switch Role** to switch back to your account.

### 5.4 Switching Roles (by a Delegated Party)

When an account establishes a trust relationship between itself and your account, you become a delegated party. You and all the users you have authorized can switch to the delegating account and manage resources under the delegated permissions.
Prerequisites

- A trust relationship has been established between another account and your account.
- You have obtained the names of the delegating account and created agency.

Procedure

**Step 1** Log in to the system as the user created in [Step 3].

**NOTE**

The user created in [Step 3] can switch roles to manage resources for the delegating party.

**Step 2** Click the logged-in account in the upper right corner of the page and choose **Switch Role**.

**Step 3** On the **Switch Role** page, enter the name of the delegating account.

**NOTE**

The system automatically matches the account to an agency. If the matched agency has not been delegated, you have no permissions to access the account. However, you can remove the agency and select an authorized one from the drop-down list box.

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

--- End
6 Federated Identity Authentication

6.1 Advantages of Federated Identity Authentication

If you have an identity authentication system, you do not need to recreate users in the SP system and can configure federated identity authentication to allow users in your system to access cloud resources directly through SSO.

Federated identity authentication is required for browser-based WebSSO or non-browser-based API calling access to the cloud system.

- **WebSSO**: A browser is used as a communication media and can be used by common users to access the cloud system.
- **API calling**: A development tool or an application is used as a communication media, for example, OpenStackClient, which is applicable to enterprises or users who use development tools to call APIs to access the cloud system.

API calling has the SP-initiated and IdP-initiated federated identity authentication modes. Users can select a mode supported by the enterprise IdP system.

**Without Federated Identity Authentication**

- Enterprise IdP users cannot log in to the cloud system through SSO.

The enterprise IdP is the IdP system of an enterprise management system. Users authenticated by their enterprise IdP cannot access the cloud system directly.

*Figure 6-1 User authentication model (1)*
User management is complex.
The enterprise administrator has to create accounts separately in the enterprise management system and the cloud system.

User operations are complex.
Users have to use different accounts to log in to the enterprise management system and cloud system.

**Figure 6-2 User login model (1)**

With Federated Identity Authentication

- IdP users can log in to the cloud system through SSO.

Any user authenticated by the enterprise IdP can access the cloud system directly. The enterprise administrator does not need to create separate users in the cloud system.

**Figure 6-3 User authentication model (2)**
User management is more convenient.
The enterprise administrator does not need to create separate users in the cloud system, reducing the cost of personnel management.

User operations are simplified.
Users can access both the enterprise management system and the cloud system simply by logging in to the enterprise management system.

Figure 6-4 User login model (2)

6.2 Configuring Federated Identity Authentication
Federated identity authentication allows enterprise users to access the cloud system after being authenticated by the enterprise IdP.

**NOTICE**
The enterprise IdP server and the cloud system must use the same Universal Time Coordinated (UTC) time. Any time inconsistency will cause federated identity authentication failure.

Step 1 Establish a trust relationship between the cloud system and the enterprise IdP. For details, see section Establishing a Trust Relationship.
**Step 2** On the IAM console, create an IdP. For details, see section *Creating an IdP*.

**Step 3** On the IAM console, specify permissions for the enterprise IdP users to access the cloud system. For details, see section *Using Rules to Control Federated User Access to the Cloud System*.

**Figure 6-6** User conversion model

**Step 4** Configure a login link for the cloud system in the enterprise management system to achieve SSO. For details, see section *Configuring SSO*.

**Figure 6-7** SSO configuration model
After logging in to the enterprise management system, enterprise IdP users can click the login link to access the resources in the cloud system.

**Step 5** Configure the client or development tool to call APIs to access the cloud system.

---End

### 6.3 Establishing a Trust Relationship

Establish a trust relationship between the two systems by exchanging metadata files.

**Step 1** Download the metadata file of the cloud system. If a user needs to use both Web Single Sign-On (WebSSO) and API calling functions, the user has to download the metadata files of both the WebSSO and the API.

- **WebSSO:** Visit [https://auth.huaweicloud.com/authui/saml/metadata.xml](https://auth.huaweicloud.com/authui/saml/metadata.xml) and [https://auth.prod-cloud-ocb.orange-business.com/authui/saml/metadata.xml](https://auth.prod-cloud-ocb.orange-business.com/authui/saml/metadata.xml) and [https://auth.otc.t-systems.com/authui/saml/metadata.xml](https://auth.otc.t-systems.com/authui/saml/metadata.xml). Right-click, choose **Save As**, and set a file name, for example, **websso-metadata.xml**.

- **API calling:** Visit [https://Endpoint address of a region/v3-ext/auth/OS-FEDERATION/SSO/metadata](https://Endpoint address of a region/v3-ext/auth/OS-FEDERATION/SSO/metadata), right-click on the page and choose **Save As**, and set a file name, for example, **api-metadata-region.xml**.

  The cloud system provides API gateways depending on the region for users to call APIs. To access multiple regions, a user needs to download metadata files of the corresponding regions.

**Step 2** Obtain the metadata file of the enterprise IdP. For details about how to obtain this file, contact the administrator of the enterprise management system.

**Step 3** Upload the metadata file of the cloud system to the enterprise IdP server. For details about how to upload the file, contact the administrator of the enterprise management system.

**Step 4** Upload the metadata file of the enterprise IdP to the IAM server. For details, see section **Creating an IdP**.

---End

### 6.4 Creating an IdP

After an IdP is created on IAM and the metadata file of the IdP is configured, users authenticated by the enterprise IdP can access the cloud system directly.

**Context**

In IAM, federated identity authentication only supports the SAML 2.0 protocol, so the enterprise IdP must support SAML 2.0 to use federated identity authentication.

Security Assertion Markup Language (SAML) is an XML-based open standard for exchanging authentication and authorization data between security domains. You can visit [https://en.wikipedia.org/wiki/SAML_2.0](https://en.wikipedia.org/wiki/SAML_2.0) for more information about SAML 2.0.
Prerequisites

A trust relationship has been established between the two systems. For details, see section Establishing a Trust Relationship.

Procedure

**Step 1** In the navigation pane, choose Identity Providers.

**Step 2** On the Identity Providers page, click Create Identity Provider.

**Step 3** Set Name, Status, and Description for the IdP.

**NOTE**
Currently, only the SAML protocol is supported.

**Step 4** Click OK.

If the information shown in Figure 6-8 is displayed, the IdP has been created successfully.

**Figure 6-8 IdP created successfully**

Identity provider created successfully. Go to the Modify Identity Provider page to complete your identity provider information.

**Step 5** Configure IdP information by clicking the Modify Identity Provider link before the IdP list page is displayed. Alternatively, click Modify in the Operation column of the row that contains the target IdP after the IdP list page is displayed.

**Step 6** In the Metadata Configuration area on the Modify Identity Provider page, configure the metadata using either of the following method:

- **Upload metadata**
  The system supports uploading and manual configuration of metadata. If the metadata file size exceeds 500 KB, you can click the manually configure link to configure it. If metadata is updated subsequently, you need to upload or edit metadata. Otherwise, federated users cannot log in to the cloud system.
  - **Upload metadata.**
    - **Click next to Upload, and select the metadata file of the enterprise IdP.**
    - **Click Upload.**
      A dialog box is displayed, showing the metadata extracted by the system.
    - **Click OK.**
      - If "The uploaded file contains multiple IdPs. Select an IdP as needed." is displayed, select the desired IdP from the Entity ID drop-down list box.
      - If a message is displayed indicating that Entity ID in the metadata file is empty or that the signature certificate has expired, check whether the metadata file is correct. Then, upload the file again or configure the metadata manually.
iv. Click **OK**.
   - Manually configure metadata.
   i. Click **manually configure**.
   ii. On the displayed **Manually Configure Metadata** page, enter **Entity ID**, **Signature Certificates**, **SingleSignOnService**, and other parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity ID</td>
<td>An entity ID uniquely identifies an enterprise IdP. A metadata file can contain multiple IdPs. You need to select your desired IdP.</td>
</tr>
<tr>
<td>Supported Protocols</td>
<td>The SAML protocol is used for federation identity authentication between the enterprise IdP and the SP. IAM only supports SAML 2.0.</td>
</tr>
<tr>
<td>Supported NameIdFormat</td>
<td><strong>Supported NameIdFormat</strong> defines the name identifier formats supported by the IdP. Name identifiers can be used for communication between the IdP and the federated users.</td>
</tr>
<tr>
<td>Signature Certificates</td>
<td>A signature certificate is used to verify the signatures and contains a public key. For security purposes, a 2048-bit public key is recommended. During federated identity authentication, the system checks the credibility and integrity of an assertion based on the signature certificate in the metadata file.</td>
</tr>
<tr>
<td>SingleSignOnService</td>
<td>This is how SAML requests are sent during the SSO process. <strong>SingleSignOnService</strong> must support HTTP Redirect or HTTP POST.</td>
</tr>
<tr>
<td>SingleLogoutService</td>
<td>The SP provides the session logout function. After a federated user logs out of a session from IAM, the user is redirected to the address that was bound to its account. <strong>SingleLogoutService</strong> must support HTTP Redirect or HTTP POST.</td>
</tr>
</tbody>
</table>

iii. Click **OK**.

**Step 7** Click **OK** to save the settings.

---End

**Verification**

**Step 1** Click **View** in the row that contains the target IdP.

**Step 2** Click **Copy** to the right of **Login link** to copy the address in **Login link**, and then open it using a browser.

**Step 3** Check whether the login page provided by the enterprise IdP server is displayed.
NOTE
If the redirection fails, check whether the obtained enterprise metadata file and the enterprise IdP server are configured correctly.

Step 4 Enter a username and API password and check whether you can log in to the cloud system.

End

Follow-up Procedure

- In the Identity Conversion Rule area, create an identity conversion rule. For details about identity conversion rules, see Using Rules to Control Federated User Access to the Cloud System.
- Configure SSO in the enterprise management system. For details, see Configuring SSO.

Related Operations

- Viewing IdP information
  In the IdP list, click View to query basic information, metadata details, and identity conversion rules for the corresponding IdP.
  NOTE
  You can click Modify Identity Provider on the View Identity Provider page to enter the Modify Identity Provider page.

- Modifying IdP information
  In the IdP list, click Modify to enter the Modify Identity Provider page. You can set Status (Enabled or Disabled), Description, Metadata File, and Identity Conversion Rule.

- Deleting an IdP
  In the IdP list, click Delete in the row that contains the target IdP to delete it.

6.5 Configuring SSO

Configuring an IdP login link on the enterprise management system allows enterprise users to access the cloud system after being authenticated by the enterprise IdP.

Prerequisites

An IdP has been created, and its login link is available.

Procedure

Step 1 In the navigation pane, choose Identity Providers.

Step 2 Click View in the row that contains the target IdP.

Step 3 Click Copy to the right of Login link.

Step 4 On the web page of the enterprise management system, press F12 and configure the following information:

<cloud-system-entry>
After logging in to the enterprise management system, enterprise users can click the system entry link on the enterprise management system to access the cloud system.

---End

6.6 Using Rules to Control Federated User Access to the Cloud System

The enterprise administrator uses the enterprise IdP to manage the identities and permissions of federated users. An identity conversion rule is used to map the identities and permissions of federated users to those in the cloud system. The cloud system uses the rule to control which operations federated users can perform and which resources they can access.

Prerequisites

- An IdP has been created, and its login link is available.
- You have a preliminary understanding of the SAML 2.0 protocol and are familiar with metadata files.
- You have learned the assertion structure displayed after successful SAML 2.0 authentication.

Procedure

**Step 1** In the navigation pane, choose **Identity Providers**.

**Step 2** In the identity provider list, click **Modify** in the row that contains the IdP you have created.

The **Modify Identity Provider** page is displayed.

**Step 3** In the **Identity Conversion Rule** area, click **Create Rule** to add an identity conversion rule.

**NOTE**

After an IdP is created successfully, the cloud system will preconfigure a default rule. This rule converts the usernames of federated users to **FederationUser**, which is displayed in the cloud system. This rule only allows the federated users in the current IdP to access certain resources. If this default rule does not meet your requirements, you can click **Edit Rule** to modify it.
Username: indicates the username displayed in the cloud system after a federated user logs in. You are advised to enter a username that starts with FederationUser_ to differentiate between users in the cloud system and federated users. You can also enter a simple expression, such as FederationUser_{email}. After this rule is created successfully, the system automatically replaces {email} with the email address of the
The username displayed in the cloud system is \texttt{FederationUser\_XXX@XXX}. \texttt{XXX@XXX} indicates the email address of the federated user. This rule only takes effect if the assertion contains an email address.

- **User Group**: indicates the user group to which the federated user belongs after logging in to the cloud system. The user's permissions are determined by their user group.

- **Conditions for Validating This Rule**: indicates the conditions under which the federated user has the permissions of the selected user groups. When these conditions are met, the federated user has the permissions of their user group. If these conditions are not met, the rule does not take effect, and users who do not meet these conditions are not allowed to access the cloud system.

For example, set a rule for an enterprise system administrator:

- **Username**: FederationUser\_admin\_\{email\}
- **User Group**: admin
- **Conditions for Validating This Rule** (\texttt{Attribute: \_NAMEID; \texttt{Condition: any\_one\_of; Value: ID1;ID2;ID3}}): The rule takes effect only for the users of the specified IDs. Only the users whose user IDs are ID1, ID2, or ID3 have the permissions of the admin user group in the cloud system. The other users of this IdP do not have these permissions.

\textbf{NOTE}

- Multiple effective conditions can be set for a rule. The rule will take effect as long as any of these conditions is met.
- Multiple rules can be created for an IdP. These rules take effect at the same time. If none of the created rules take effect for a federated user, the user is not allowed to access the cloud system.

\textbf{Step 4} In the Create Rule area, click \textbf{OK}.

\textbf{Step 5} On the Identity Providers page, click \textbf{OK} for the settings to take effect.

\textbf{Related Operations}

- Viewing rules: In the Identity Conversion Rule area, click \textbf{View Rule}. The newly created identity conversion rule is displayed in a JSON file. For details about its content, see section \textbf{Identity Conversion Rule for Federated Users}.

- Editing rules: In the Identity Conversion Rule area, click \textbf{Edit Rule}. This function provides flexible syntax for editing rules to meet the federated identity authentication requirements. For examples of rules, see section \textbf{Identity Conversion Rule for Federated Users}.

\textbf{NOTE}

After the rules are edited, you can click \textbf{Verify Rule} in the lower left corner of the page to verify that they are correct.

\section*{6.7 Identity Conversion Rule for Federated Users}

The identity conversion rule for federated users is displayed in a JSON file. You can modify it by modifying the JSON file. The JSON format is as follows:

```
[  {    "remote": [}
```
remote: indicates the information about a federated user in the IdP. This expression is a combination of assertion attributes and operators. The value of remote is determined based on the assertion.

condition: indicates the identity conversion rule that maps federated users to the cloud system. The following three conditions are supported:

- empty: unlimited. The condition is always valid and the returned value is the input attribute value. This value is used to replace the placeholder in the local block.
- any_one_of: The condition is valid only if the input attributes include any specified value, and a Boolean value is returned. The returned value cannot be used to replace the placeholder in the local block.
- not_any_of: The condition is valid only if the input attributes do not include any specified value, and a Boolean value is returned. The returned value cannot be used to replace the placeholder in the local block.

local: indicates the information about a federated user in the cloud system. This value can be a placeholder \{0..n\}. \{0\} indicates the first attribute of the user information in remote. \{1\} indicates the second attribute of the user information in remote.

Examples of Identity Conversion Rule Conditions

The following examples illustrate how to use the conditions (empty, any_one_of, and not_any_of) in an identity conversion rule.

The empty condition indicates that a character string value can be returned. This value is used to replace the placeholder \{0..n\} in the local block. The example is as follows:

```json
{
    "<condition>",
    "local": [
        {
            "<user> or <group> or <groups>"
        }
    ]
}
```
The username of the federated user in the cloud system is "first attribute value of remote + space+ second attribute value of remote", or FirstName LastName. The belonged user group is the third attribute value of remote, that is Group. The Group attribute can have only one value.

Assume that the cloud system receives the following assertion (this example uses a simplified assertion structure). The username of the federated user in the cloud system is John Smith. John Smith in the cloud system is attached to the admin user group.

```json
{FirstName: John}
{LastName: Smith}
{Groups: admin}
```

If a federated user needs to belong to multiple user groups in the cloud system, the identity conversion rules are as follows:

```json
[
  {
    "local": [
      {
        "user": {
          "name": "{0} {1}"
        }
      },
      {
        "groups": "{2}"
      }
    ],
    "remote": [
      {
        "type": "FirstName"
      },
      {
        "type": "LastName"
      },
      {
        "type": "Groups"
      }
    ]
  }
]
```

The username of the federated user in the cloud system is "first attribute value of remote + space + second attribute value of remote", or FirstName LastName. The user group of the federated user is the third attribute value of remote, that is Groups.

Assume that the cloud system receives the following assertion, the username of the federated user in the cloud system is John Smith. John Smith belongs to the admin and manager user groups.

```json
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```

- Unlike the empty condition, the returned values of the any one of and not any of conditions are Boolean values. These values cannot be used to replace the placeholder in the local block. In the following example, only the placeholder {0} exists and is replaced by the returned value of empty in the remote block. The value of group must be admin.

```json
[
  {
    "local": [
      {
        "user": {
          "name": "{0}"
        }
      }
    ]
  }
]```
The username of the federated user in the cloud system is the first attribute value of `remote`, that is **UserName**. The user group of the federated user is **admin**. This rule takes effect only for the users in the **idp_admin** user group in the IdP.

If a federated user needs to belong to multiple user groups in the cloud system, the identity conversion rules are as follows:

```json
{
    "local": [
        {
            "user": {
                "name": "{0}""            
            }
        },
        {
            "groups": "["admin","manager"]"
        }
    ],
    "remote": [
        {
            "type": "UserName"
        },
        {
            "type": "Groups",
            "any_one_of": [
                "idp_admin"
            ]
        }
    ]
}
```

The username of the federated user in the cloud system is the first attribute value of `remote`, that is **UserName**. The user groups of the federated user are **admin** and **manager**. This rule takes effect only for the users in the **idp_admin** user group in the IdP.

- Assume that the cloud system receives the following assertion. John Smith belongs to the **idp_admin** user group and can therefore access the cloud system.
  ```json
  {UserName: John Smith}
  {Groups: [idp_user, idp_admin, idp_agency]}
  ```

- Assume that the cloud system receives the following assertion. John Smith does not belong to the **idp_admin** user group, so this rule does not take effect for John Smith, and John Smith cannot access the cloud system.
  ```json
  {UserName: John Smith}
  {Groups: [idp_user, idp_agency]}
  ```
• Condition including a regular expression: You can specify "regex": true in conditions to indicate that the system is calculating the result using a regular expression.

```json
{
    "local": [
        {
            "user": {
                "name": "[0]"
            }
        },
        {
            "group": {
                "name": "admin"
            }
        }
    ],
    "remote": [
        {
            "type": "UserName"
        },
        {
            "type": "Groups",
            "any_one_of": [
                ".*@mail.com$"
            ],
            "regex": true
        }
    ]
}
```

This rule takes effect for any user whose username starts with any value and ends with @mail.com. The username in the cloud system is **UserName**, and the user group is **admin**.

• Condition combination: Multiple conditions are combined using the logical AND.

```json
{
    "local": [
        {
            "user": {
                "name": "[0]"
            }
        },
        {
            "group": {
                "name": "admin"
            }
        }
    ],
    "remote": [
        {
            "type": "UserName"
        },
        {
            "type": "Groups",
            "not_any_of": ["idp_user"
        ],
        {
            "type": "Groups",
            "not_any_of": ["idp_agent"
        ]
    ]
}
```
This rule takes effect only for the federated users who do not belong to the idp_user or idp_agent user group in the IdP. The username of those users in the cloud system is UserName, and their user group is admin. The preceding rule is equivalent to the following:

```
[
  {
    "local": [{
      "user": {
        "name": "{0}""
      }
    }, {
      "group": {
        "name": "admin"
      }
    }],
    "remote": [{
      "type": "UserName"
    }, {
      "type": "Groups",
      "not_any_of": [{
        "idp_user",
        "idp_agent"
      }]
    }]
  }
}
```

**Multiple rules**

If multiple rules are combined, the methods for generating usernames and user groups are different.

The username in the first valid rule is used as UserName. At least one user name rule among all of the rules must take effect, or the user will not be allowed to log in. The collection of the user group names in all valid rules is used as Groups.

Separating the configuration of usernames and user groups using multi-rule configuration makes it easier to read.

```
[
  {
    "local": [{
      "user": {
        "name": "{0}""
      }
    }],
    "remote": [{
      "type": "UserName"
    }]
  },
  {
    "local": [{
      "group": {
        "name": "admin"
      }
    }],
    "remote": [
```

```
This rule combination takes effect for the users in the `idp_admin` user group. The username in the cloud system is `UserName`, and the user group is `admin`.

Assume that the cloud system receives the following assertion. John Smith belongs to the `idp_admin` user group, so this rule takes effect for John Smith. The username of the federated user in the cloud system is `John Smith`, and its user group is `admin`.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```

### 6.8 SSO Process

After federated identity authentication is configured, federated users can access the cloud system directly and manage resources in the system by logging in to the enterprise IdP. This section describes how IAM authenticates a federated user after the user is authenticated by the IdP.
**Figure 6-11 Login process model**

![Diagram of the login process model](image)

**Description**

**NOTE**

To view the interactive requests and assertion information more easily, you are advised to use the Google Chrome web browser and install the SAML Message Decoder plug-in.

1. Open the login link generated after an IdP is created in a web browser. The web browser initiates SSO.
2. IAM finds the metadata file of the enterprise IdP based on the account and IdP carried in the link and constructs a SAML Request to respond to the web browser.
3. The web browser responds and forwards the SAML Request to the enterprise IdP.
4. Users enter a username and password on the IdP server for identity authentication.
5. The IdP server constructs an assertion in a SAML Response to respond to the web browser.
6. The web browser responds and forwards the SAML Response to IAM.
7. IAM extracts the assertion from the SAML Response and parses the assertion. Based on the configured rules, IAM generates a token to implement the login.
NOTE

The assertion must carry a signature or the login will fail.
7 Security Credential Management

7.1 Viewing Security Credentials

You need to use security credentials when you access the system through the management console or APIs, or perform service interconnection in the system. You can view security credentials on the My Credentials page.

Procedure

**Step 1** On the console page, click the username in the upper right corner and select My Credential from the drop-down list.

**Step 2** On the My Credentials page, view the basic account information.

<table>
<thead>
<tr>
<th>Basic Information</th>
<th>Description</th>
</tr>
</thead>
</table>
| Username          | Username used for logging in to the system.  
- The username created in MyWorkplace is in the following format: ICU userid Contract instance number.
- The username created in Open Telekom Cloud is user-defined. |
| User ID           | Unique identifier for a user in the system. It is automatically generated by the system. |
| Account Name      | Name of an account domain. An account domain refers to an entity that bears expenses, for example, an enterprise. It is automatically created during registration. Cloud service resources are isolated by account domain.  
**Domain Name** is the same as the username created in MyWorkplace, that is, ICU userid Contract instance name. The name is required when you log in to the system. |
| Domain Name       | |

Table 7-1 Basic account information
### Basic Information

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account ID</strong></td>
</tr>
<tr>
<td><strong>Domain ID</strong></td>
</tr>
<tr>
<td>Unique identifier for an accounta domain in the system. The account IDdomain ID is automatically generated by the system.</td>
</tr>
<tr>
<td><strong>Verified Email Address</strong></td>
</tr>
<tr>
<td>Email address bound to a user. You can use your email address to log in to the system, reset your passwords, and receive verification codes and other push notifications.</td>
</tr>
<tr>
<td><strong>Verified Mobile Number</strong></td>
</tr>
<tr>
<td>Mobile number bound to a user. You can use your mobile number to log in to the system, reset their passwords, and receive verification codes and other push notifications.</td>
</tr>
<tr>
<td><strong>API Password</strong></td>
</tr>
<tr>
<td>Login password configured in the system.</td>
</tr>
<tr>
<td><strong>Verify Login by SMS Message</strong></td>
</tr>
<tr>
<td>Whether SMS message-based login authentication is enabled. If it is enabled, you need to enter an SMS verification code when attempting to log in.</td>
</tr>
<tr>
<td><strong>Login Authentication Method</strong></td>
</tr>
<tr>
<td>IAM provides three login authentication methods: virtual MFA-based login authentication, SMS-based login authentication, and email-based login authentication. After login authentication is enabled, you need to enter an authentication code from a virtual MFA device, an SMS verification code, or an email verification code on the <strong>Login Verification</strong> page in addition to the username and password when logging in to the system.</td>
</tr>
<tr>
<td><strong>Virtual MFA Device</strong></td>
</tr>
<tr>
<td>You can enable the virtual MFA-based login authentication function only when a virtual MFA device is bound to your account.</td>
</tr>
<tr>
<td><strong>Project</strong></td>
</tr>
<tr>
<td>Projects are used to group and isolate OpenStack resources, including computing, storage, and network resources. Your resources must be mounted under projects. A project can be a department or a project team. You can create projects in a region to perform isolated management of resources.</td>
</tr>
<tr>
<td><strong>Project List</strong></td>
</tr>
<tr>
<td>List of projects an account can access. The project parameter needs to be specified when you access native OpenStack APIs.</td>
</tr>
<tr>
<td><strong>Access Keys</strong></td>
</tr>
<tr>
<td>AK/SK. A maximum of two pairs can be created. The AK/SK is used to encrypt the signature when accessing the system through APIs.</td>
</tr>
</tbody>
</table>

---

### 7.2 Modifying Security Credentials

You can modify your own credential information, such as the verified email address, API password, and avatar. To ensure information security, you are advised to change the API password periodically and enable **Verify Login by SMS Message** and enable the login authentication function.
Context

If you are a user of another system, that is, a user not generated after registration in this system, you need to enter the login password when using SDK or calling APIs, set the password for logging in to the system by clicking Forgot Password on the login page.

Procedure

**Step 1** On the console page, click the username in the upper right corner and select My Credential from the drop-down list.

**Step 2** On the My Credentials page, modify the information as required.

The method for changing a verified mobile number or a password is similar to that for changing a verified email address. The following is an example of how to change a verified email address.

- **Verified Email Address**
  a. Click Change to the right of Verified Email Address. The Change Email Address page is displayed.
  b. In the Verify Identity step, select the verification mode Verify by email or Verify by mobile.
  c. In the Verify Identity step, click Get Code.
  d. Enter the verification code.
  e. Click Next.
  f. In the Change Email Address step, enter New Email Address and Email Verification Code.
  g. Click OK to save the modifications.

- **Verify Login by SMS Message**
  a. Click Change. In the Set Short Message-based Login Verification dialog box, enter your SMS verification code.
  b. Click OK.
  c. **Verify Login by SMS Message** is enabled.
  d. **NOTE**
     - This function is disabled by default. You can enable this function only when you have bound both an email address and a mobile number to your account.
     - After this function is enabled, you need to enter an SMS verification code on the Login Verification page when logging in to the system.

- **Login Authentication Method**
  a. Click Modify. On the Modify Login Protection page, select a login authentication method, and enter the corresponding code.
  b. Click OK.

The login authentication method is modified successfully.
NOTE
- You can enable the virtual MFA-based login authentication function only when a virtual MFA device is bound to your account.
- After the login authentication function is enabled, you need to enter an authentication code from a virtual MFA device, an SMS verification code, or an email verification code on the Login Verification page when logging in to the system.
- To disable login authentication, select Disable for Login Authentication Method, and click OK.

● Avatar
  a. Click Change below your avatar picture.
  The Change Avatar page is displayed.
  b. Click Upload and select a picture.
  c. Click OK.
  The avatar is changed successfully.

----End

7.3 Managing Access Keys

The access key ID (AK) and secret access key (SK) are a pair of access keys used together to authenticate users who make API requests. The AK/AS pair provides similar functions as the password. When you make API requests to manage cloud resources (for example, creating a VPC), the AK and SK are required to sign the requests. This mechanism ensures the confidentiality and integrity of the requests as well as the correctness of the identities of both parties.

Procedure

Step 1 On the console page, click the username in the upper right corner and select My Credential from the drop-down list.

Step 2 On the My Credentials page, click the Access Keys tab. The created access keys are displayed.

Step 3 Manage access keys.
  ● Add and download an access key.
    a. Click Add Access Key below the list.
    
    NOTE
    Each user can create a maximum of two access keys, which are valid permanently. To ensure account security, keep them securely.
    b. Enter API Login Password and Verification Code.
    c. Click OK to generate and download the access key.
  ● Delete an access key.
    a. Click Delete.
    b. Enter API Login Password and Verification Code.
    c. Click OK.
If an access key is used improperly (for example, an access key is missing or is leaked), you must delete it immediately or contact the administrator to reset it.

Deleted access keys cannot be restored.

---End

### 7.4 Querying a Project ID

A project ID is the ID of the region where a system is located. When you access the system through APIs to perform operations on cloud resources (for example, creating a VPC), you must provide a project ID.

**Procedure**

**Step 1** On the console page, click the username in the upper right corner and select **My Credential** from the drop-down list.

**Step 2** On the **My Credentials** page, click the **Project List** tab and view **Project ID** on this tab page.

---End
Open Cloud Service Alliance users can be redirected from the management console of the hosted cloud to the management console of an allied cloud to use the resources and services of the allied cloud. Resources used by Open Cloud Service Alliance users on the allied cloud in regions outside China are charged on HUAWEI CLOUD.

**Context**

- **Open Cloud Service Alliance**: The alliance is established between carriers to implement resource and network sharing among alliance members.
- **Hosted cloud**: If a user signs an Open Cloud Service Alliance agreement with a carrier (for example, HUAWEI CLOUD), HUAWEI CLOUD is the hosted cloud of the user.
- **Allied cloud**: In Open Cloud Service Alliance, a cloud other than the hosted cloud is called the allied cloud.
- **Open Cloud Service Alliance users**, including accounts and IAM users, can be automatically synchronized to the allied cloud using the system mapping method. Registering accounts again or recreating users is not required.
- **If an Open Cloud Service Alliance user belongs to the default user group **admin** on the hosted cloud, the user also belongs to the default user group **admin** on the allied cloud. If a user belongs to a custom user group on the hosted cloud, a user group with the same name as the custom user group must be created on the allied cloud and related permissions (permissions can be different from that of the custom user group on the hosted cloud) must be granted to the created user group. After a user switches to the allied cloud, the user automatically inherits the permissions of the user group with the same name as the user group on the allied cloud.
- **The resources on the hosted cloud and the allied cloud are isolated. The resources on one cloud can be managed independently from those on the other cloud. The resources on the allied cloud are billed on the hosted cloud.**

**Prerequisites**

You have subscribed to Open Cloud Service Alliance.

**NOTE**

For details about how to subscribe to Open Cloud Service Alliance, contact the customer service personnel.
Procedure

Step 1  Log in to the hosted cloud as a user who has subscribed to Open Cloud Service Alliance. The user belongs to the default user group admin.

Step 2  On the homepage of the hosted cloud system, click Console.

Step 3  Select the partner cloud to log in to its management console without entering a password.

**NOTE**

You cannot directly log in to the allied cloud using your hosted cloud accountdomain.

The user belongs to the default user group admin on the allied cloud.

Step 4  On the management console of the allied cloud, choose Management & Deployment > Identity and Access Management.

Step 5  In the navigation pane, choose User Groups.

Step 6  On the User Groups page, click Create User Group.

**NOTE**

On the allied cloud, an Open Cloud Service Alliance user only needs to create a user group with the same name as that on the hosted cloud, and does not need to create a user with the same name.

Step 7  Enter a user group name.

The user group name must be the same as the name of the user group on the hosted cloud.

Step 8  (Optional) Set Description.

**NOTE**

It is recommended that you set Description for a user group. For example, if you grant the Security Administrator permission to a user group, you can add a description to enable users to directly view their permissions and permission details. You can add a custom description or the following description to the Description text box: Security Administrator: has the rights to create, delete, and modify users as well as grant permissions to users.

Step 9  Click OK.

The user group list is displayed, including the newly created user group.

Step 10  Click Modify in the Operation column of the row that contains the newly created user group.

The Modify User Group page is displayed.

Step 11  In the User Group Permissions area, click Modify in the Operation column of the row that contains the target project.

**NOTE**

- The permissions granted to the user group only take effect for the current project. If you need to grant the permissions for multiple projects to the user group, you must grant permissions for each project individually by clicking Modify in the row that contains the corresponding project.
- A user group does not need to have the same permissions on the allied cloud and hosted cloud. This means if a user group has the permissions in project A on the hosted cloud, it can have the permissions in project B on the allied cloud.

Step 12  In the Modify Policy dialog box, select target policies.

Step 13  Click OK.
After a user belonging to the custom user group on the hosted cloud switches to the allied cloud, the user automatically inherits the permissions of the user group with the same name as the user group on the allied cloud.

**NOTE**

- An Open Cloud Service Alliance user cannot change personal information on the allied cloud. The user can change information such as the email address, mobile number, and password on the hosted cloud.
- When an Open Cloud Service Alliance user manages cloud service resources (for example, accessing OBS) on the allied cloud, the user needs to use the access key to encrypt signatures. For details, see section *How Do I Obtain an Access Key on the Allied Cloud?*

--- End
## Change History

### Table 9-1 Change history

<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2019-01-22  | Incorporated the following change:  
Added section **Assigning Permissions (by a Delegated Party)**. |
| 2018-08-30  | This issue is the fourteenth official release.  
Incorporated the following change:  
- Added section **Using an Allied Cloud**.  
- Added the description about **Session Timeout Policy** in **Setting Account Security Policies**. |
| 2018-06-29  | This issue is the thirteenth official release.  
Incorporated the following change:  
- Added description about the **Require Password Reset** option in sections **Creating a User** and **Viewing and Modifying User Information**.  
- Added section **IAM Operations That Can Be Recorded by CTS**.  
- Added section **Viewing Audit Logs**. |
| 2018-04-30  | This issue is the twelfth official release.  
Incorporated the following change:  
- Added section **Fine-grained Policy**.  
- Added section **Policy Language**.  
- Added section **Creating Custom Policies**. |
| 2018-02-13  | This issue is the eleventh official release.  
Incorporated the following change:  
Added a table that describes agency types in **Creating an Agency (by a Delegating Party)**. |
<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-12-15</td>
<td>This issue is the tenth official release. Incorporated the following change: Deleted chapter &quot;Permission Description.&quot; For details, see Permission Description.</td>
</tr>
<tr>
<td>2017-07-27</td>
<td>This issue is the ninth official release. Incorporated the following change: Added the description for automatically extracting metadata and manually configuring metadata in Creating an IdP.</td>
</tr>
<tr>
<td>2017-06-28</td>
<td>This issue is the eighth official release. Incorporated the following change:</td>
</tr>
<tr>
<td></td>
<td>• Modified the description for the Server Administrator permission.</td>
</tr>
<tr>
<td></td>
<td>• Modified the description for the VPC Administrator permission.</td>
</tr>
<tr>
<td>Released On</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2017-05-19</td>
<td>This issue is the seventh official release. Incorporated the following change:</td>
</tr>
<tr>
<td></td>
<td>- Added the following content:</td>
</tr>
<tr>
<td></td>
<td>- Section Establishing a Trust Relationship</td>
</tr>
<tr>
<td></td>
<td>- Section SSO Process</td>
</tr>
<tr>
<td></td>
<td>- Description for the APM Admin permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the CCS Administrator permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the CCS User permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the CDE Admin permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the CDE Developer permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the SvcStg Admin permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the SvcStg Developer permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the SvcStg Operator permission</td>
</tr>
<tr>
<td></td>
<td>- Description for the SWR Admin permission</td>
</tr>
<tr>
<td></td>
<td>- Modified the description for the RDS Administrator permission.</td>
</tr>
<tr>
<td></td>
<td>- Deleted the description for the following permissions:</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_project_admin</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_project_poweruser</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_project_readonly</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codehub_admin</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codehub_poweruser</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codehub_readonly</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codecheck_admin</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codecheck_poweruser</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codecheck_readonly</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codeci_admin</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codeci_poweruser</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_codeci_readonly</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_test_admin</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_test_poweruser</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_test_readonly</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_release_admin</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_release_poweruser</td>
</tr>
<tr>
<td></td>
<td>- te_develcloud_release_readonly</td>
</tr>
<tr>
<td>Released On</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2017-04-27</td>
<td>This issue is the sixth official release.</td>
</tr>
<tr>
<td></td>
<td>Incorporated the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added section Creating an Agency (by a Delegating Party).</td>
</tr>
<tr>
<td></td>
<td>• Added section Assigning Permissions (by a Delegated Party).</td>
</tr>
<tr>
<td></td>
<td>• Added the description for the DWS Administrator permission.</td>
</tr>
<tr>
<td>2017-03-30</td>
<td>This issue is the fifth official release.</td>
</tr>
<tr>
<td></td>
<td>Incorporated the following change:</td>
</tr>
<tr>
<td></td>
<td>• Modified the descriptions in section Creating a User according to the changes in the Create User page.</td>
</tr>
<tr>
<td></td>
<td>• Added the description for the Agent Operator permission.</td>
</tr>
<tr>
<td></td>
<td>• Added the description for the CRS Administrator permission.</td>
</tr>
<tr>
<td>2016-11-30</td>
<td>This issue is the fourth official release.</td>
</tr>
<tr>
<td></td>
<td>Incorporated the following change:</td>
</tr>
<tr>
<td></td>
<td>• Modified the description in Setting Account Security Policies according to the changes in the Account Policy page.</td>
</tr>
<tr>
<td>2016-09-30</td>
<td>This issue is the third official release.</td>
</tr>
<tr>
<td></td>
<td>Incorporated the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added section Creating an IdP.</td>
</tr>
<tr>
<td></td>
<td>• Added section Using Rules to Control Federated User Access to the Cloud System.</td>
</tr>
<tr>
<td>2016-08-25</td>
<td>This issue is the second official release.</td>
</tr>
<tr>
<td></td>
<td>Incorporated the following change:</td>
</tr>
<tr>
<td></td>
<td>• Added the settings of the Minimum Password Validity Period (Minutes) parameter.</td>
</tr>
<tr>
<td>2016-03-14</td>
<td>This issue is the first official release.</td>
</tr>
</tbody>
</table>