Organizations

User Guide

Issue 01

Date 2025-12-10





Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions

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

Notice

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

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

Contents

1 Permissions Management	1
1.1 Creating an IAM User and Granting Organizations Permissions	1
1.2 Creating Custom Policies	2
2 Managing Organizations	4
2.1 Overview of Organizations	
2.2 Creating an Organization	4
2.3 Viewing Details About an Organization	5
2.4 Deleting an Organization	7
3 Managing OUs	9
3.1 Overview of an OU	g
3.2 Creating an OU	9
3.3 Modifying an OU	11
3.4 Viewing Details About an OU	11
3.5 Deleting an OU	12
4 Managing Accounts	14
4.1 Overview of an Account	14
4.2 Inviting an Account to Join Your Organization	15
4.3 Creating an Account	19
4.4 Closing an Account	23
4.5 Moving an Account	24
4.6 Viewing Account Details	25
4.7 Removing a Member Account from Your Organization	26
4.8 Viewing Account Invitation/Creation Records	29
5 Managing SCPs	32
5.1 Overview of an SCP	32
5.1.1 SCP Introduction	32
5.1.2 SCP Principles	33
5.1.3 SCP Syntax	37
5.2 Enabling or Disabling the SCP Type	40
5.3 Creating an SCP	41
5.4 Modifying or Deleting an SCP	45
5.5 Attaching or Detaching an SCP	46

5.6 Example SCPs	40
5.7 System-defined SCPs	
5.8 Cloud Services for Using SCPs	
5.9 Regions for Using SCPs	
6 Managing Tag Policies	
6.1 Overview of a Tag Policy	
6.2 Tag Policy Syntax	
6.3 Enabling or Disabling the Tag Policy Type	
6.4 Creating a Tag Policy	
6.5 Viewing the Effective Tag Policy	
6.6 Editing or Deleting a Tag Policy	
6.7 Attaching or Detaching a Tag Policy	
6.8 Cloud Services for Using Tag Policies	
6.9 Regions for Using Tag Policies	76
7 Managing Trusted Services	78
7.1 Overview of a Trusted Service	78
7.2 Enabling or Disabling a Trusted Service	79
7.3 Trusted Services for Organizations	81
7.4 Specifying, Viewing, or Removing a Delegated Administrator	91
8 Managing Tags	94
8.1 Overview of a Tag	94
8.2 Adding a Tag	96
8.3 Editing a Tag	97
8.4 Viewing Tag Details	99
8.5 Deleting a Tag	99
9 CTS Auditing	102
9.1 Supported Organizations Operations	
9.2 Viewing CTS Traces in the Trace List	
10 Adjusting Quotas	113

Permissions Management

1.1 Creating an IAM User and Granting Organizations Permissions

This section describes how a management account creates an IAM user and grants organization administrator permissions to the user.

You can use Identity and Access Management (IAM) for fine-grained permissions control on Organizations. With IAM, you can:

- Grant users only the permissions required to perform a given task based on their job responsibilities. For example, you use the management account to create two IAM users, and assign one of them the permissions to create and delete OUs while the other one only the permission to view information about OUs.
- Use the management account to create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials to access Huawei Cloud and use Organizations, improving account security.
- Entrust another Huawei Cloud account or a cloud service to perform efficient O&M on your Organizations.

If your HUAWEI ID or Huawei Cloud cloud account meets your permissions requirements, you can skip this section.

The following describes how to create an IAM user and grant permissions to the user. Figure 1-1 illustrates an example process.

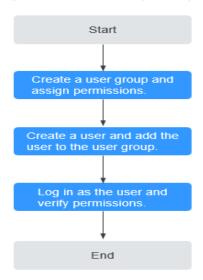
Prerequisites

Before assigning permissions to user groups, learn about the permissions supported by Organizations, as described in Permissions.

For the permissions of other services, see System Permissions.

Process Flow





- On the IAM console, Create a user group and assign permissions.
 Create a user group on the IAM console to assign the **Organizations ReadOnlyAccess** permission to the group.
- Create an IAM user and add it to the user group.
 Create a user on the IAM console and add it to the user group created in 1.
- 3. Log in and verify permissions.

Log in to the Organizations console as the IAM user. If you can access Organizations and view organization information but encounter an error message when you attempt to add an OU, saying "Insufficient permission. Contact the administrator", the **Organizations ReadOnlyAccess** policy has been applied and you have only the permission to view organization information.

1.2 Creating Custom Policies

You can create custom policies to supplement the system-defined policies of Organizations. For the actions that can be added to custom policies, see Policies and Supported Actions.

To create a custom policy, choose either visual editor or JSON.

- Visual editor: Select cloud services, actions, resources, and request conditions. There is no need to know much about policy syntax.
- JSON: Edit policies from scratch or based on an existing policy in JSON format.

For details, see Creating a Custom Policy. The following lists examples of common Organizations custom policies.

Example Custom Policies

• Example 1: Grant permission to invite member accounts to join an organization or to remove member accounts from an organization.

```
{

"Version": "5.0",

"Statement": [

{

    "Effect": "Allow",

    "Action": [

    "organizations:accounts:invite",

    "organizations:accounts:remove"

    ]

}

]
```

• Example 2: Grant permission to deny the deletion of OUs or removal of member accounts.

To apply a policy with only Deny statements, it must be used together with other policies. If you do not assign the permission to perform an action, the action is denied by default. If the permissions granted to an IAM user contain both Allow and Deny, the Deny statements take precedence over the Allow statements.

Assume that you want to grant the permissions of the **OrganizationsFullAccess** policy to a user but want to prevent them from deleting OUs or removing member accounts. You can create a custom policy for denying the deletion, and attach this policy together with the **OrganizationsFullAccess** policy to the user. As an explicit Deny in any policy overrides any kind of Allow, the user can perform all operations on a given organization except deleting its OUs or removing member accounts. The following is an example of a deny policy:

2 Managing Organizations

2.1 Overview of Organizations

What Is Organizations?

An organization is an entity that you create to manage multiple accounts. Each organization is composed of exactly one management account, multiple member accounts, and one root with many OUs organized in a hierarchical, tree-like structure. You can group member accounts into the root or any of the OUs. For details about the basic concepts of Organizations, see Basic Concepts.

Helpful links:

- Creating an Organization: You can use your current account as the management account to create an organization and invite other accounts to join your organization.
- **Viewing Details About an Organization**: You can view details about your organization, root, OUs, and accounts.
- **Deleting an Organization**: You can delete an organization when you no longer need it.

2.2 Creating an Organization

You can use a Huawei Cloud account as the management account to create an organization. After creating the organization, you can **invite existing accounts** or **create new accounts** to add them to your organization, and you can **create OUs** to manage accounts in your organization.

Prerequisites

The current account has not joined any organization. If this account is already in an organization and you still need to use it, remove it from the current organization and then use it to create your organization. For how to remove from an organization, see Leaving an Organization As a Member Account.

The current account must have enabled Enterprise Center and become an enterprise master account. For details, see Enabling Enterprise Center.

Procedure

You can create an organization on the management console or by calling Organizations APIs. The following describes how to create an organization on the console.

- **Step 1** Log in to Huawei Cloud and access the Organizations console.
- **Step 2** Go to the page for enabling the Organizations service, and click **Enable Organizations**.

Figure 2-1 Enabling Organizations



After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account.

After the Organizations service is enabled, the management account cannot be transferred to any other Huawei Cloud account/HUAWEI ID.

----End

Then, you can invite existing accounts to join your organization or create new accounts in your organization, and you can also create OUs to manage accounts.

2.3 Viewing Details About an Organization

You can use the management account to view all information about your organization. The member accounts can view only the organization ID, management account name, and management account ID.

Viewing Organization Details from the Management Account

Log in to the Organizations console as an organization administrator or using the management account. On the **Settings** page, you can view the organization ID, URN, management account name, and management account ID.

Organizations Settings Organization **Organization Details** Accounts Organization ID rknp 🗇 Policies URN 5ad88f5ef6a4bcffc:organization:o-doxbpkzgsdd51ti1k27w2v8fitakrknp Services Settings Management Account Name Management Account ID Delete Organization You can delete an organization only after you remove all member accounts and organizational units and detach all policies from the organization. Learn more

Figure 2-2 Viewing organization details from the management account

Viewing Root Details from the Management Account

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Click the organization root. You can view details about the root on the right of the organization tree, including the root ID, time of creation, URN, policies, and tags.

----End

Viewing OU Details from the Management Account

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Click the OU. You can view details about the OU on the right of the organization tree, including the OU name, ID, URN, when the OU was created, as well as policies and tags attached.

----End

Viewing Account Details from the Management Account

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Click the account. You can view details about the selected account on the right of the organization tree, including the account name, account ID, URN, time when the account joined the organization, parent OU, as well as policies, tags, and agency services associated with the account.

Viewing Organization Details from a Member Account

Log in to the Organizations console as a member account. On the **Settings** page, you can view the organization ID, URN, management account name, and management account ID.

2.4 Deleting an Organization

Prerequisites

You can delete an organization when you no longer need it.

□ NOTE

An organization can be deleted only after all member accounts, OUs, and policies are removed from the organization.

Impacts

• Impacts on the Management Account

- The management account will become a standalone account. You can
 use it to create a different organization or accept an invitation from
 another organization to add the account to that organization as a
 member account.
- The management account of an organization is never affected by service control policies (SCPs). There is no change to the permissions assigned to the management account and its IAM users.

Impact on Member Accounts

- Each member account will become a standalone account. You can use it to create a different organization or accept an invitation from another organization to add the account to that organization as a member account.
- After the organization is deleted, member accounts are no longer affected by SCPs, and the permissions assigned to the member accounts and their IAM users may change.

• Impact on Policies

 If you delete an organization, you cannot recover it. If you have created SCPs inside the organization, they are also deleted and you cannot recover them.

Procedure

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account and access the **Settings** page.
- **Step 2** Click **Delete Organization**. In the displayed dialog box, click **OK**.

Figure 2-3 Deleting an organization



3 Managing OUs

3.1 Overview of an OU

What Is an OU?

An organizational unit (OU) is a container or a logical grouping of accounts in your organization. You can use OUs to group accounts together to administer them as a single unit. An OU can be mapped to a department, a subsidiary, or a project team. You can create OUs within other OUs. Each OU can have only one parent OU, but they can have many other child OUs or member accounts.

Helpful links:

- Creating an OU
- Modifying an OU
- Viewing Details About an OU
- Deleting an OU

3.2 Creating an OU

You can create an OU in your organization's root. OUs can be nested up to five levels deep.

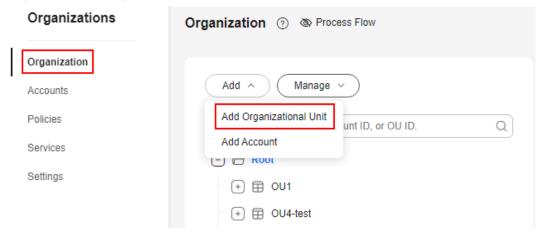
To create an OU:

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the parent OU by clicking its name rather than the expand icon. If you are creating an OU for the first name, select the **Root** OU.

OUs can be nested up to five levels deep. Each OU can have only one parent OU but can have many child OUs. When creating an OU, ensure that the parent OU you select is the upper-level one.

Step 3 Choose Add > Add Organizational Unit.

Figure 3-1 Adding an OU



- **Step 4** In the displayed dialog box, enter the OU name.
- Step 5 (Optional) Add a tag to the OU.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for OUs. A maximum of 20 tags can be added to an OU.

Table 3-1 describes the key and value descriptions of a tag.

Table 3-1 Tag description

Elem ent	Description	Example
Tag key	A tag key of an OU must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS).	Key_0001
	A tag key:	
	• Cannot be an empty string.	
	• Contains 1 to 128 characters.	
	 Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF). 	
Tag value	A tag value can be repetitive or an empty string.	Value_0001
ratae	A tag value:	
	Can be an empty string. Contains 1 to 225 characters.	
	• Contains 1 to 225 characters.	
	 Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF). 	

Step 6 Click OK.

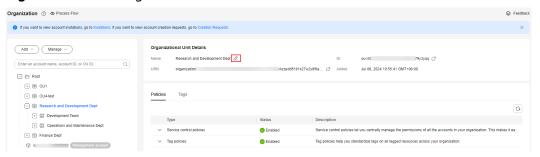
3.3 Modifying an OU

After an OU is created, you can modify its name, tag, and policy at any time. For details about how to modify tags and policies, see **Managing Tags** and **Attaching or Detaching an SCP**.

Procedure

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU you want to rename and click an next to the OU name on the displayed OU details page.

Figure 3-2 Renaming an OU



Step 3 Enter a new name for the OU and click \checkmark to save it.

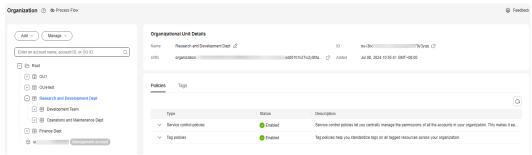
----End

3.4 Viewing Details About an OU

After an OU is created, you can view its details any time by following the steps below.

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Click the OU you want to view. Its details are displayed on the right of the OU tree, including the OU name, ID, URN, time of creation, policies, and tags.

Figure 3-3 Viewing details about an OU



----End

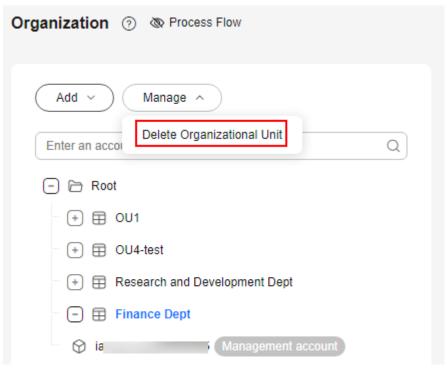
3.5 Deleting an OU

You can delete an OU that is no longer needed.

You cannot delete an OU if it contains other OUs or accounts.

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Click the OU you want to delete and click **Manage** above the OU tree.
- Step 3 Choose Delete Organizational Unit. In the displayed dialog box, click OK.

Figure 3-4 Deleting an OU



4 Managing Accounts

4.1 Overview of an Account

Accounts in Your Organization

An account is used to contain your Huawei Cloud resources. It is the smallest unit of an organization. Each organization has one management account and multiple member accounts.

Table 4-1 Account types

Account Type	Function	Quota
Manage ment account	With the Organizations service, you can use the management account to create an organization and manage OUs, accounts, and policies for the organization.	1 (Each organization can have exactly one management account.)
Member account	Except for the management account, other accounts in an organization are member accounts. Each member account is part of only one organization at a time. Generally, member accounts hold resources for a specific application or project of an organization.	9

Impacts of Being in an Organization

When you invite an existing account to your organization or create a new account in your organization, Organizations will automatically make the following changes to the new member account:

 A service-linked agency is created in the member account. It is a cloud service agency with the system-defined permission
 OrganizationsServiceLinkedAgencyPolicy for all resources.

- The permissions of the new member account are affected by service control
 policies and tag policies. You may have service control policies and tag policies
 attached to the root or the OU that contains the new member account. If so,
 the policies will apply to the new member account and all IAM users in the
 member account.
- When you use the management account to enable a trusted service, the trusted service can create a service-linked agency for that trusted service in the member account

Helpful links:

- **Inviting an Account to Join Your Organization**: You can create invitations, manage invitations you have sent, and accept or reject invitations.
- Creating an Account: You can use the management account to create new accounts.
- Closing an Account: You can use the management account to close any unwanted accounts that you have created. Invited accounts cannot be closed.
- Moving an Account: You can move accounts from one OU to another OU.
- **Viewing Account Details**: You can view the account name, account ID, the time when it joined an organization, any account-owing OUs, and the policies, tags, and delegated services that are attached to the account.
- Removing a Member Account from Your Organization: You can use the management account to remove member accounts from your organization.
- Viewing Account Invitation/Creation Records: When you sign in to the
 management account of your organization, on the Accounts page, you can
 view account details, including the account list, creation records, and
 invitations. You can also invite, create, close, move, and remove accounts and
 cancel any pending invitations.

4.2 Inviting an Account to Join Your Organization

When you invite a HUAWEI ID or Huawei Cloud account to join your organization, Organizations sends an invitation to the ID or account owner, who then chooses to accept or reject the invitation. You can use the Organizations console to issue and manage invitations that you send to other accounts.

□ NOTE

The accounts you invite to join your organization must have completed enterprise or individual real-name authentication. For details, see Real-Name Authentication.

The original accounting relationship (master-member association) of invited accounts will remain unchanged.

This section includes the following content:

- Issuing Invitations to Accounts
- Managing Open Invitations of Your Organization
- Accepting or Rejecting an Invitation from an Organization

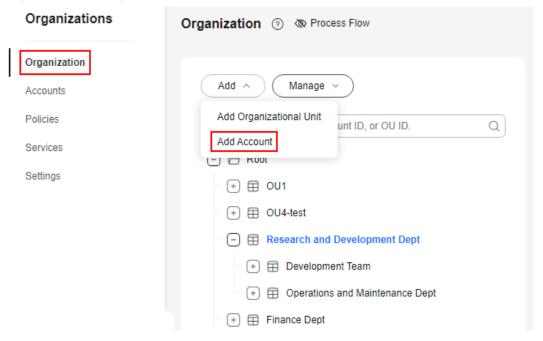
Issuing Invitations to Accounts

To invite other accounts to join your organization, perform the steps described in this section. By default, those invited accounts will be placed as member accounts

in the root OU. If you want to move them to another OU, see **Moving an Account**.

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** On the **Organization** page, choose **Add > Add Account**.

Figure 4-1 Adding an account



Step 3 In the displayed dialog box, select **Invite existing** and enter the name or ID of the account you want to invite.

For details about how to obtain an account name or ID, see Obtaining Account ID and Name.

Add Account You can add an account to your organization either by inviting an existing account or by creating an account. Invite existing Create new ★ Account ② Account ID 3c24f6f8 :e075fbd use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags Q Tags to add a tag, ettler a lag key and a tag value below. Enter a tag value Add Enter a tag key Tags you can still add: 20 Cancel

Figure 4-2 Inviting an existing account

Step 4 (Optional) Add one or more tags to the account.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for accounts. You can add up to 20 tags to an account.

Table 4-2 describes the key and value descriptions of a tag.

Table 4-2 Tag description

Elem ent	Description	Example
Tag key	A tag key of an account must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS).	Key_0001
	A tag key:	
	• Cannot be an empty string.	
	• Contains 1 to 128 characters.	
	 Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF). 	
Tag	A tag value can be repetitive or an empty string.	Value_0001
value	A tag value:	
	Can be an empty string.	
	• Contains 1 to 225 characters.	
	 Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF). 	

Step 5 Click **OK** to send an invitation to the invited account.

----End

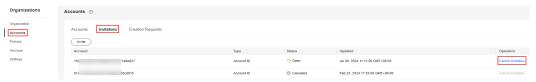
Managing Open Invitations of Your Organization

When you log in as the management account, you can view and manage invitations of your organization.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account and access the **Accounts** page.
- **Step 2** Click the **Invitations** tab. You can view all the invitations sent from your organization and their statuses on the page.
- **Step 3** Locate the **Open** invitation you want to cancel and click **Cancel Invitation** in the **Operation** column. Then, click **OK** in the displayed dialog box.

After the invitation is canceled, its status changes from **Open** to **Canceled**. If you want that account to join your organization again, you must send a new invitation.

Figure 4-3 Canceling an invitation



----End

Accepting or Rejecting an Invitation from an Organization

Your account may receive an invitation to join an organization. You can accept or reject the invitation.

◯ NOTE

Each account can join only one organization. If you receive multiple invitations, you can accept only one of them. If you have joined an organization, you need to exit that organization before accepting an invitation from another organization.

- **Step 1** Log in to the Organizations console as the invited member account.
- **Step 2** Locate the target invitation and click **Accept** or **Decline** in the **Operation** column. Then, click **OK** in the displayed dialog box.

Figure 4-4 Accepting or rejecting an invitation



4.3 Creating an Account

You can use the management account to create new accounts in your organization. The accounts you created are referred to as resource accounts. For details, see What Are the Differences Between a Resource Account and a Cloud Account in the Unified Accounting Model? If you want to convert a resource account to a cloud account, refer to Converting a Resource Account to a Huawei Cloud Account.

This section includes the following content:

- Creating an Account
- Logging In with the New Account Via an Agency
- Logging In with the New Account via IAM Identity Center

Constraints

- An organization administrator can create a maximum of five accounts at a time.
- Accounts created via Organizations can be used for login only by switching roles via an agency or by accessing the IAM Identity Center console.
- The accounting of accounts created via Organizations is hosted by the organization management account by default.

<u>A</u> CAUTION

 An agency will be created in the new account created via Organizations for the management account. You can delete this agency in the new account. Before deleting the agency, enable IAM Identity Center and configure related identities and permissions to ensure that the service owner can access the account.

Creating an Account

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** On the **Organization** page, choose **Add > Add Account**.

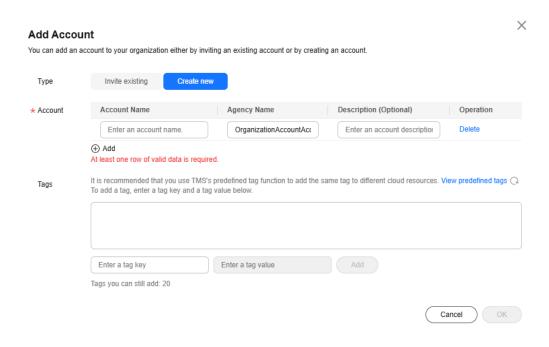
Organizations Organization ② 🚳 Process Flow Organization Add ^ Manage Accounts Add Organizational Unit Policies unt ID, or OU ID. Q Add Account Services □ K001 Settings ⊕ ⊕ 0U1 (+) ⊞ OU4-test - Research and Development Dept + Development Team + Department of the Property o + Finance Dept

Figure 4-5 Adding an account

- **Step 3** Click **Create new** in the displayed dialog box.
- **Step 4** Enter an account name. You can enter the account description as required. The account name must be unique.

You can retain the default agency name or change it as required.

Figure 4-6 Creating an account



Step 5 (Optional) Add one or more tags to the account.

A tag consists of a key-value pair. Tags are used to identify, classify, and search for accounts. You can add up to 20 tags to an account.

Table 4-3 describes the key and value descriptions of a tag.

Table 4-3 Tag description

Elem ent	Description	Example
Tag key	A tag key of an account must be unique. You can create a custom key or select a key of an existing tag created in Tag Management Service (TMS).	Key_0001
	A tag key:Cannot be an empty string.	
	Contains 1 to 128 characters.	
	 Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF). 	
Tag value	A tag value can be repetitive or an empty string.	Value_0001
	A tag value:Can be an empty string.	
	Contains 1 to 225 characters.	
	 Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF). 	

Step 6 Click **OK**. The new account is added to the list.

----End

Logging In with the New Account Via an Agency

Step 1 Hover over the username in the upper right corner and click **Others**. The role switching page is displayed.

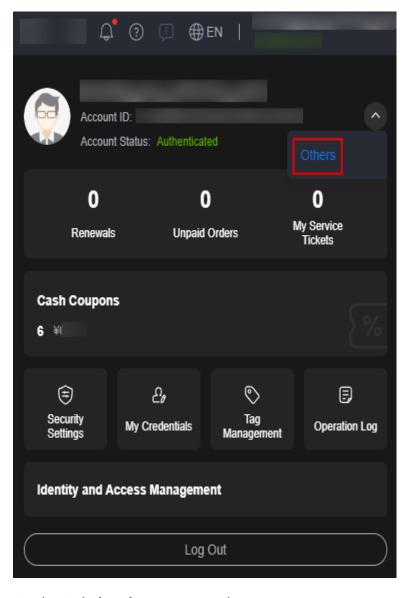
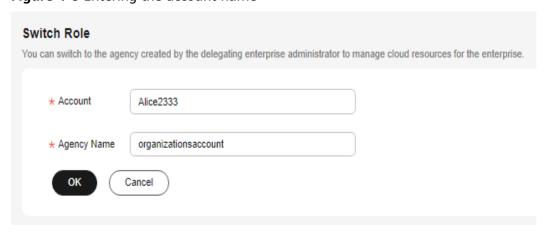


Figure 4-7 Switching the role

Step 2 On the **Switch Role** page, enter the account name.

Figure 4-8 Entering the account name



After you enter the account name, the agencies created under this account will be automatically displayed when you click the agency name text box. An agency name starting with **cbc**_ will also be displayed. This agency is mainly used by an enterprise master account to centrally manage expenditures and grant permissions to member accounts. You need to select the agency name entered when creating the account.

Step 3 Click **OK** to switch to the account.

----End

Logging In with the New Account via IAM Identity Center

After an account is created, you can associate it with users and permission sets in IAM Identity Center. Then, you can log in to the Organizations console through the user portal URL of IAM Identity Center and access resources of the account in the organization. The specific access permission for resources is controlled by the permission set in IAM Identity Center.

- **Step 1** Associating Accounts with Users/Groups and Permission Sets
- **Step 2** Logging In as an IAM Identity Center User and Accessing Resources

----End

4.4 Closing an Account

If you no longer need a member account, you can close it from the management account of your organization following the instructions in this section. If you want to close the management account, you have to delete your organization. For details, see **Deleting an Organization**.

⚠ CAUTION

- Once your request to close an account is submitted, data in the account will start to be deleted and cannot be restored. This operation cannot be undone.
- After the data in an account is deleted, the account status changes to Closed.
 The account will be retained in the account list for 90 days before being permanently deregistered.

Constraints

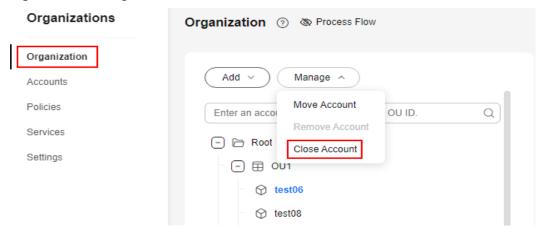
- You can close accounts you created but not those you invited to your organization.
- If any accounts you created have become cloud accounts, they cannot be closed.
- Any account that is specified as a delegated administrator cannot be closed unless you remove the delegated administrator first, as described in Removing a Delegated Administrator.

- The management account can only close 10% of the member accounts (no more than 200 accounts) in a given organization within 30 days, and no more than three at a time.
- The mobile number or email address associated with the closing account cannot be used to create another account.
- Any account that has prepaid resources, generally yearly/monthly resources, cannot be closed unless you confirm and unsubscribe from such resources, as described in Unsubscribing from In-Use Resources.
- Any account that has resources in arrears cannot be closed unless you top up your account and pay off the arrears, as described in Top-Up and Payment.

Procedure

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the account you want to close and choose **Manage** > **Close Account**.

Figure 4-9 Closing an account



- **Step 3** In the displayed dialog box, read and confirm the risks of closing the account, and enter the account name to reconfirm the operation.
- Step 4 Click OK.
 - ----End

4.5 Moving an Account

When you log in as the management account, you can move an account from one OU to another.

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the account you want to move, and choose **Manage** > **Move Account**.

Organizations Organization ② ® Process Flow Organization Add ~ Manage ^ Accounts Move Account Policies Enter an accor OU ID. Q Remove Account Services — Root Close Account Settings — □ 0U1 test06

test08

Figure 4-10 Moving an account

Step 3 Select the OU you choose to hold the account, and enter "Confirm" in the text box. Then, click **OK**.

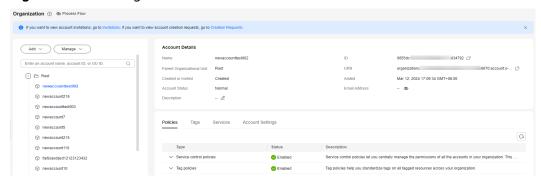
----End

4.6 Viewing Account Details

You can view the details of accounts in your organization at any time by following the steps below.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account and access the **Organization** page.
- **Step 2** Select the account you want to view. Its details are displayed in the pane on the right, including the account name, ID, home OU, URN, how and when the account joined the organization, when the account was created, account status, email address, account description, as well as policies, tags, and deleted services.

Figure 4-11 Viewing account details



4.7 Removing a Member Account from Your Organization

Precautions

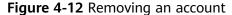
Before the organization administrator removes a member account from an organization or before a member account leaves an organization, it is important to know the following:

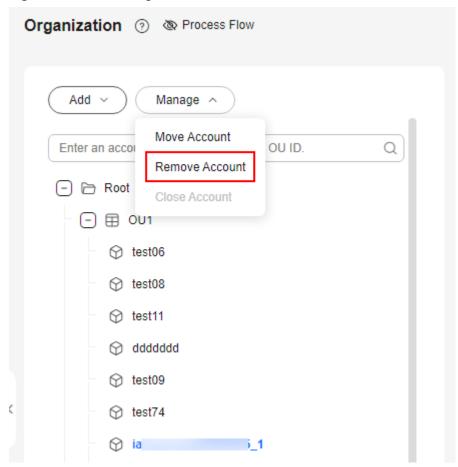
- The member account in question has to have been created more than seven calendar days ago.
- The account has to have been converted to a Huawei Cloud account. For details, see Converting a Resource Account to a Huawei Cloud Account.
- Invited accounts can be removed from or leave an organization only if they are Huawei Cloud accounts. For details, see Differences Between Resource Accounts and Huawei Cloud Accounts.
- A delegated administrator account cannot be removed from or leave an organization. You need to remove the delegated administrator first. For details, see Removing a Delegated Administrator.
- After an account created via Organizations leaves an organization, the IAM
 agency created by default during the creation of the account will not be
 automatically deleted. The organization management account can still use
 that agency to access data of member accounts. To prevent unauthorized
 access, you need to manually delete the agency. For details, see Deleting an
 Agency.
- After an account created via Organizations leaves the organization, the
 accounting relationship between the account and the organization
 management account remains unchanged. After an account that was invited
 to join an organization leaves the organization, its original accounting
 relationship remains unchanged. For details about how to disassociate a
 member account, see Disassociating Member Accounts.
- After a member account leaves an organization, the permissions assigned by the organization policies will no longer apply. This means that the account may actually have more permissions than before. If you enabled trusted access for a cloud service, the account can no longer use the functions of that trusted service.
- When a member account leaves an organization, all tags attached to the account are deleted.

Removing an Account

When you sign in to the management account of your organization, you can remove member accounts that you no longer need. The following steps apply only when you remove member accounts. If you want to remove the management account, you must delete the organization by following the instructions in **Deleting an Organization**.

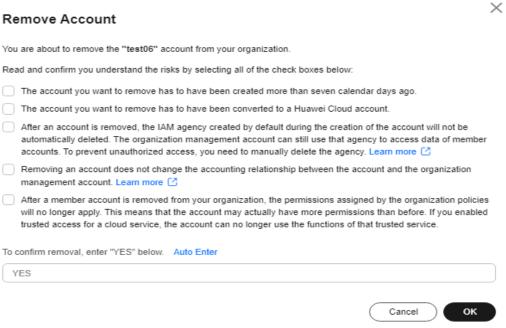
- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the account you want to remove, and choose **Manage** > **Remove Account**.





Step 3 In the displayed dialog box, read and confirm you understand the risks by selecting all of the check boxes, and then enter **YES** and click **OK**.

Figure 4-13 Confirming the risks of removing the account



----End

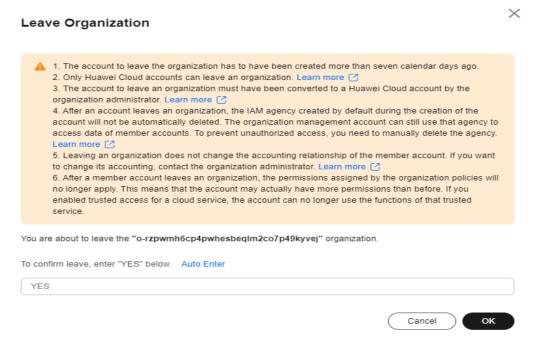
Leaving an Organization As a Member Account

When you sign in to a member account of an organization, you can choose to leave the organization. The management account cannot leave the organization using this method. To remove the management account, you must delete the organization by referring to **Deleting an Organization**.

Any account that is specified as a delegated administrator cannot leave an organization unless you remove the delegated administrator first, as described in **Removing a Delegated Administrator**.

- **Step 1** Log in to the Organizations console as a member account.
- **Step 2** On the **Settings** page, click **Leave Organization**. In the displayed dialog box, read and confirm you understand the risks, and then enter **YES** and click **OK**.

Figure 4-14 Confirming the risks of leaving the organization



----End

4.8 Viewing Account Invitation/Creation Records

When you sign in to the management account of your organization, on the **Accounts** page, you can view account details, including the account list, creation records, and invitations. You can also invite, create, close, move, and remove accounts and cancel any pending invitations.

This section includes the following content:

- Viewing the Account List
- Viewing Invitations
- Viewing Creation Requests

Viewing the Account List

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** Access the **Accounts** page, and click the **Accounts** tab.

In the account list, you can view the details of all the accounts in your organization.

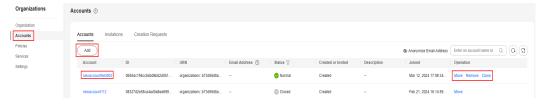


- **Step 3** Click an account name in the list to view its details.
- **Step 4** Click **Move**, **Close**, or **Remove** in the **Operation** column.

You cannot close any accounts that have been invited to your organization.

Step 5 Click **Add** in the upper left corner of the list. In the displayed dialog box, you can invite existing accounts to join your organization or create new accounts in the organization.

Figure 4-15 Account list



----End

Viewing Invitations

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Accounts** page, click the **Invitations** tab.

You can view the details about account invitations.

- **Step 3** Click **Cancel Invitation** in the **Operation** column to cancel an invitation in the **Open** state.
- **Step 4** Click **Invite** in the upper left corner of the list. In the displayed dialog box, you can invite existing accounts to join your organization.

Figure 4-16 Invitations



----End

Viewing Creation Requests

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Accounts** page, click the **Creation Requests** tab.

You can view the details about account creation requests.

Step 3 Click **Create Account** in the upper left corner of the list. In the displayed dialog box, you can create new accounts for your organization.

Figure 4-17 Creation requests



5 Managing SCPs

5.1 Overview of an SCP

5.1.1 SCP Introduction

What Are Service Control Policies?

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. The organization management account can use SCPs to limit which permissions can be assigned to member accounts to ensure that they stay within your organization's access control guidelines. SCPs can be attached to an organization, OUs, and member accounts. Any SCP attached to an organization or OU affects all the accounts within the organization or under the OU.

Helpful links:

- SCP Principles: SCP types, how SCPs work, inheritance of SCPs, and relationship between SCPs and IAM policies
- SCP Syntax: SCP structure and parameters

Testing SCP Effects

Before applying an SCP to your production environment, it is strongly recommended that you use test accounts in a test environment first to perform thorough system design and testing. This helps avoid any unpleasant surprises in the production environment. After the SCP has been fully verified in the test environment, you can create an OU and move one or a few accounts into it at a time, to ensure that the use of resources is not inadvertently interrupted.

CAUTION

Do not detach the system-defined SCP FullAccess unless you replace it with a custom policy with allowed actions. If you detach FullAccess and configure a custom policy with allowed actions, you must configure actions required by services as well as iamToken::* and signin::*.

- If you detach the FullAccess SCP from the root OU, the operations for all accounts in the organization will fail. Exercise caution when detaching the FullAccess SCP because this operation is very risky.
- If you detach the FullAccess SCP from an OU, the operations for the accounts in that OU and its lower-level OUs will fail.
- If you detach the FullAccess SCP from a member account, the operations for that account will fail.

Tasks Not Restricted by SCPs

You cannot use SCPs to restrict the following tasks:

- Any actions performed by the organization management account or IAM users.
- Any actions performed using permissions that are attached to a service-linked agency.
- Any API calls made by SCP-unsupported cloud services to SCP-supported cloud services. For SCP-supported cloud services, see Cloud Services for Using SCPs.
- Token obtained by APIs used for access to APIs of SCP-supported cloud services (in most cases).

Helpful Links

For details about the differences in access control between IAM and Organizations, see What Are the Differences in Access Control Between IAM and Organizations?

5.1.2 SCP Principles

SCP Types

SCPs are classified as either system-defined policies or custom policies, depending on who creates them.

• System-defined policies

System-defined policies refer to commonly used SCPs predefined by Huawei Cloud services for Organizations. An organization administrator can directly use these policies when attaching SCPs to OUs or accounts. Such policies cannot be modified. For details about available SCP system policies, see **System-defined SCPs**.

Custom policies

If system-defined policies cannot meet your requirements, you can use the management account to create and modify custom SCPs based on the actions supported by each service. Custom policies extend and supplement system-defined policies. You can create custom policies for Organizations in a policy editor or JSON view.

SCP Effects on Permissions

Permissions boundaries

SCPs do not actually grant any permissions to an entity. They only set permissions boundaries for the entity. When SCPs are attached to an OU or a member account, they do not directly grant permissions to that OU or member account. Instead, the SCPs only determine what permissions are available for that member account or member accounts under that OU. The granted permissions can be applied only if they are allowed by the SCPs. Users cannot perform any actions that are denied by SCPs even if the actions are granted to the users by IAM policies.

Suppose that an SCP is attached to a member account. The SCP allows action A but denies action B. The member account then can grant its IAM users the permission to perform action A but not action B. Even if the permission to perform action B is assigned, the permission cannot be applied.

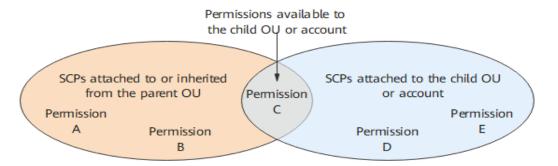
Permissions intersection

The final effective permissions of an OU or account are the intersection of the permissions of its own SCPs and the allowed SCPs of its parent OU.

In the following figure, the oval on the left represents an SCP attached to the parent OU. It allows permissions A, B, and C. The oval on the right represents an SCP attached to the child OU or account. It allows permissions C, D, and E. Because the SCP attached to the parent OU does not allow permission D or E, no child OUs or accounts under the parent OU can use them. Even though the SCP attached to the child OU explicitly allows permissions D and E, they are blocked by the SCP attached to the parent OU. Because the SCP attached to the child OU or account does not allow permission A or B, those permissions are blocked for the child OU or account. In this case, the child OU or account can actually use the permission (permission C in the following figure) in the intersection of its own permissions and the allowed permissions of its parent OU.

If the entity in the set on the right represents a member account, the set of maximum permissions that can be granted to the users and user groups in that account is the intersection of the two sets. If the entity represents a child OU, then the set of maximum permissions that can be granted to that OU is the intersection of the two sets.

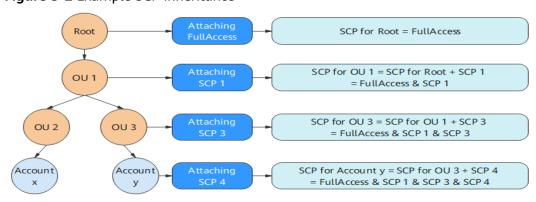
Figure 5-1 How SCPs work



Policy inheritance

SCPs for an OU or account can be attached directly or inherited from the root OU or the parent OU. When you attach an SCP to a specific OU, all child OUs and accounts under that OU will inherit that policy. The permissions boundaries of an account or an OU are determined by a combination of the SCPs attached to all upper-level OUs and the SCPs directly attached to the account or OU. In the following figure, Account y is nested in OU 3, and its permissions boundary is jointly determined by the SCPs inherited from the root OU and the SCPs attached to OU 1 and OU 3 as well as Account y.

Figure 5-2 Example SCP inheritance



If you want to allow a service action at the member account level, you must allow that action at every level between the member account and the root OU of your organization. Specifically, you must attach SCPs that allow the given action to every level from the root OU to the member account. You can use either a deny list or an allow list.

A deny list: This strategy uses the **FullAccess** SCP that is attached by default to every OU and account. This SCP overrides the default implicit Deny and allows all permissions to flow down from the root OU to every account, unless you explicitly deny a permission with an additional SCP that you create and attach to the appropriate OU or account. No account below the level of the OU with the deny policy can use the denied action, and there is no way to add the permission back lower in the hierarchy.

Allow by default

When SCPs are enabled for an organization, the **FullAccess** policy is attached by default to all OUs and accounts unless you attach explicit deny policies to the OUs or accounts.

Differences Between Explicit Deny and Implicit Deny

The effect of Deny indicates the permission to deny an operation.

If there are no applicable Deny statements, all requests are denied by default. This is called an implicit deny.

If a policy includes an applicable Deny statement, requests will be denied. This is called an explicit deny.

The following figure shows the logic for authenticating an access request.

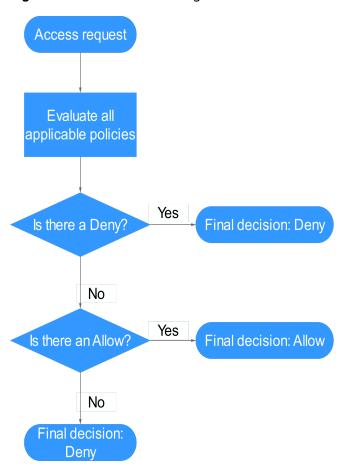


Figure 5-3 Authentication logic

- 1. A principal sends an access request.
- 2. The system looks for a Deny statement that applies to the request. If the system finds an applicable Deny, it returns a final decision of Deny, and the authentication ends.
- 3. If no applicable Deny is found, the system looks for an Allow that would apply to the request. If the system finds an applicable Allow, it returns a final decision of Allow, and the authentication ends.
- 4. If no applicable Allow is found, the system returns a final decision of Deny, and the authentication ends.

5.1.3 SCP Syntax

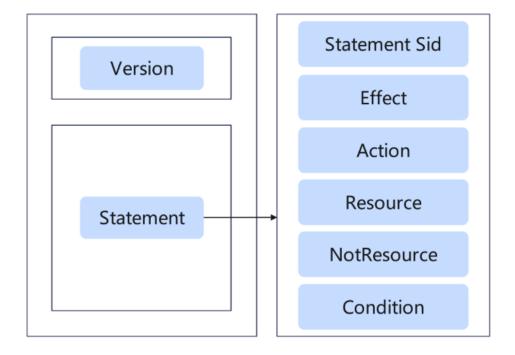
The following uses a custom policy for RAM as an example to describe the SCP syntax.

SCPs use a similar syntax to that used by IAM identity policies.

Policy Structure

A policy consists of a version and a single statement or an array of individual statements, each indicating a different action.

Figure 5-4 Policy structure



Policy Elements

The following table describes the policy elements (Version and Statement).

Table 5-1 Policy elements

Element		Manda tory	Description	Value
Version		Yes	Policy version.	5.0 (cannot be customized)
Stateme nt: Permissi ons defined by a	Stateme nt ID (Sid)	No	Identifier of a policy statement. You can assign a Sid value for each statement in a statement array.	A user-defined character string
policy	Effect	Yes	Determines whether to allow or deny the operations defined in an action.	Deny
	Action	Option al for Deny statem ents	Operations that the SCP allows or denies.	Format: "Service name:Resource type:Operation". For example, vpc:subnets:list indicates the permission to view the VPC subnet list, where vpc is the service name, subnets refers to the resource type, and list is the action.
	Conditio n	Option al for Deny statem ents	Determines when a policy is in effect. A condition consists of a condition key and a condition operator.	Format: "Condition operator:{Condition key. [Value 1, Value 2]}" If you configure multiple conditions, the policy can be applied only when all the conditions are met. Example: "StringEndWithIfExists": {"g:UserName": ["specialCharacter"]}: The statement is valid only for users whose names end with specialCharacter.

Element	Element		Description	Value
	Resource	No. If this elemen t is not specifie d, * is used by default, indicati ng that the SCP applies to all resourc es.	Resources that the SCP applies to.	The value can be either * or a specific resource for Deny statements. Format: Service name:region:domain ID:Resource type:Resource path. Wildcard characters (*) are supported, indicating all resources. Example: "ecs:*:*:instance:*", representing all ECS instances.
	NotReso urce	No. If it is not specifie d, see Resour ce.	Resources that the policy does not apply to.	

■ NOTE

The following elements are not supported in SCPs:

- Principal
- NotPrincipal
- NotAction

Condition Keys

A condition key is a key in the **Condition** element of a statement. The condition key that you specify can be a global condition key or a service-specific condition key. For details, see the condition keys supported by each service in Global Condition Keys.

Operators

A condition operator, a condition key, and a condition value together constitute a complete condition statement. A policy can be applied only when its request conditions are met. Operators can have the "IfExists" suffix added, which means the policy will take effect either if the corresponding request value does not exist or if it exists and meets the condition. For example, "StringEqualsIfExists" indicates that the policy will take effect if the request value does not exist or if it equals the condition value. For details, see Operators.

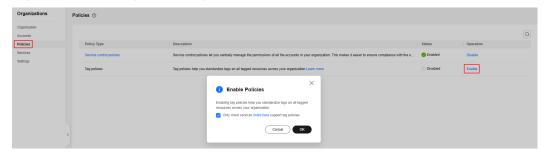
5.2 Enabling or Disabling the SCP Type

Enabling the SCP Type

Before you create and attach an SCP to OUs and accounts, you have to enable the SCP type from the organization's management account. After the SCP type is enabled, Organizations automatically attach the FullAccess policy (allowing for all operations) to all OUs and accounts.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Enable** in the **Operation** column of the service control policies.
- **Step 3** In the displayed dialog box, select the check box and click **OK**.

Figure 5-5 Enabling the SCP type



----End

Disabling the SCP type

If you no longer want to use SCPs to manage permissions for your organization, you can disable the SCP type from the organization's management account.



- After the SCP type is disabled in an organization, all SCPs are automatically detached from all OUs and accounts in the organization. However, the SCPs are not deleted.
- If you disable the SCP type and then enable it again, the FullAccess SCP is still attached to all entities in the organization and attachments of other SCPs are lost. If you want to re-enable them, you must re-attach them to the entities.
- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Disable** in the **Operation** column of the service control policies.

Figure 5-6 Disabling the SCP type



Step 3 Click **OK** in the displayed dialog box.

----End

5.3 Creating an SCP

This topic describes how to create a custom SCP. For SCP examples, see **Example SCPs**.

Constraints

- Effect in a custom SCP can only be set to Deny.
- Only Action is supported. NotAction is not supported.
- The action prefix must be the name of a cloud service that has been interconnected with IAM 5.0, for example, Action="ram:*:*". Wildcards (*) are not supported for prefixes. For example, Action="*" or Action="*:*:*" is not allowed.
- An action in a custom SCP must contain three fields and have the following structure:

Procedure

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Service control policies**.

Figure 5-7 Accessing the Service control policies page



Step 3 Click Create Policy.

[&]quot;service-name:type-name:action-name"

Figure 5-8 Creating an SCP



Step 4 Enter a policy name. Ensure that you are entering a unique policy name. It must be different from any other existing policy.

(Optional) You can also enter a description for the policy.



Step 5 On the left of the policy content, edit the policy content in JSON.

For details about how to build JSON policy statements, see **SCP Syntax** and **Example SCPs**.



Ⅲ NOTE

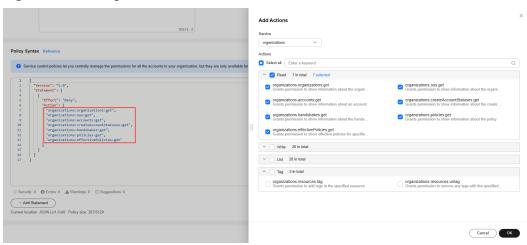
The Version value of a custom policy must be 5.0.

Step 6 Hover over the statement on the left of the policy content, and edit the actions, resources, and conditions of the custom policy in the policy editor on the right.



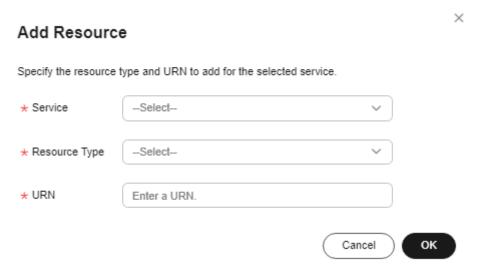
• Adding an action: You can click ⊕, and select or search for the service and action to be added. The added action will be displayed in **Action** on the left of the policy content. **Figure 5-9** shows the details.

Figure 5-9 Adding an action



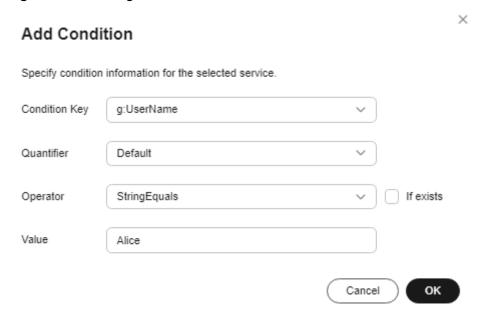
 Adding a resource: Only services available for resource-level authorization can be added. You can click to select a service and resource type and enter the URN as required, as shown in Figure 5-10.

Figure 5-10 Adding a resource



(Optional) Adding a condition: You can click
 to add a condition key and a condition operator to define the conditions for the policy to take effect, as shown in Figure 5-11.

Figure 5-11 Adding a condition



Step 7 (Optional) Click Add Statement to add an object for the Statement element.

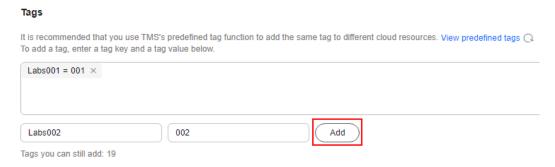
The value for the Statement element can be an array of multiple objects that identify different permissions.

Figure 5-12 Adding a statement



Step 8 (Optional) Add one or more tags. Enter a tag key and a tag value, and click **Add**.

Figure 5-13 Adding tags to the SCP



Step 9 Click **Save**. If the policy list is displayed, the SCP is created successfully. If a message appears indicating incorrect policy content, modify the SCP syntax.

----End

5.4 Modifying or Deleting an SCP

The following describes how to modify and delete a custom SCP.

Modifying an SCP

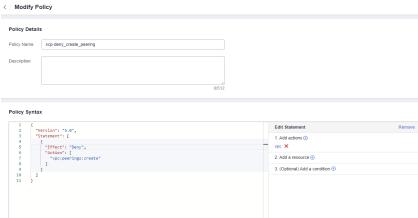
- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Service control policies**.
- **Step 3** Locate the custom SCP you want to modify and click **Edit** in the **Operation** column. In the displayed dialog box, enter "Confirm" and click **OK**.

Figure 5-14 Modifying an SCP



Step 4 On the **Modify Policy** page, modify the policy name and description as needed, as shown in **Figure 5-15**.

Figure 5-15 Modifying an SCP



- **Step 5** Edit the policy content if needed. You can use the statement editor to modify the policy syntax. For details, see **SCP Syntax**.
- **Step 6** Click **Save**. If the policy list is displayed, the SCP is updated successfully. If a message appears indicating incorrect policy content, modify the SCP syntax.

----End

Deleting an SCP

An SCP that is attached to OUs or accounts cannot be deleted. To delete such an SCP, you need to detach the SCP from the OUs or accounts first.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- Step 2 On the Policies page, click Service control policies.
- **Step 3** Locate the target custom SCP and click **Delete** in the **Operation** column.
- **Step 4** Click **OK** in the displayed dialog box.

Figure 5-16 Deleting an SCP



----End

5.5 Attaching or Detaching an SCP

You can attach an SCP to or detach it from the root OU, other OUs, or accounts from the organization's management account.

Constraints

• SCPs affect only member accounts in an organization. They have no effect on the management account, IAM users, and agencies.

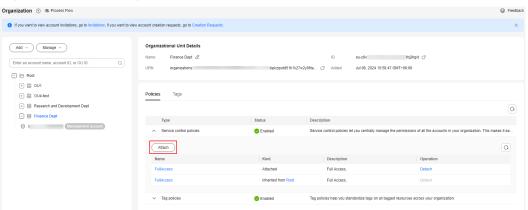
- SCPs are applied within 30 minutes after they are attached.
- You cannot attach SCPs to the organization administrator.

Attaching an SCP

Method 1:

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU or account you want to attach the SCP to.
- **Step 3** On the details page, click the **Policies** tab. On the page, expand **Service control policies** and click **Attach**.

Figure 5-17 Attaching an SCP



Step 4 Select the policy to be added and enter "Confirm" in the text box. Then, click **Attach**.

----End

Method 2:

- **Step 1** On the Organizations console, access the **Policies** page.
- **Step 2** Click **Service control policies**. The list of SCPs is displayed.
- **Step 3** Locate the SCP you want to attach and click **Attach** in the **Operation** column. Then, select the OU or account you want to attach the SCP to.
- **Step 4** In the displayed dialog box, enter "Confirm". Click **OK**.

Attach Policy

Service control policies

Create Policy

Name

Type

Condense Policy

Name

Type

Condense Policy

Condense Po

Figure 5-18 Attaching an SCP

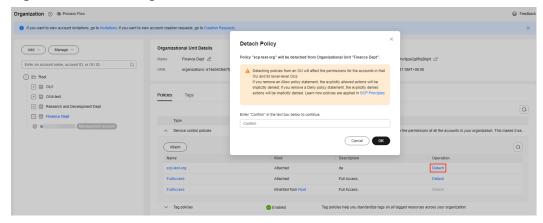
----End

Detaching an SCP

Method 1:

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU or account you want to detach the SCP from.
- **Step 3** On the details page, click the **Policies** tab. On the page, expand **Service control policies**, locate the target SCP, and click **Detach** in the **Operation** column.
- **Step 4** In the displayed dialog box, enter "Confirm". Click **OK**.

Figure 5-19 Detaching an SCP



◯ NOTE

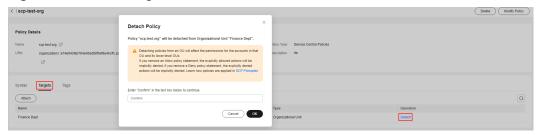
You cannot detach the last SCP from an OU or account. There must be at least one SCP attached to every OU or account.

----End

Method 2:

- **Step 1** On the Organizations console, access the **Policies** page.
- **Step 2** Click **Service control policies**. The list of SCPs is displayed.
- **Step 3** Click the name of the target SCP and click the **Targets** tab.
- **Step 4** Locate the OU or account from which the SCP is to be detached and click **Detach** in the **Operation** column. In the displayed dialog box, enter "Confirm" and click **OK**.

Figure 5-20 Detaching an SCP



----End

5.6 Example SCPs

This section provides some example SCPs for your reference, including:

- Preventing Member Accounts from Leaving an Organization
- Blocking Service Access for the Root User
- Prohibiting Creation of Resources with Specified Tags
- Prohibiting Access to Specified Regions
- Preventing Sharing with Accounts Outside an Organization
- Preventing Sharing Specified Resource Types
- Preventing Aggregation Authorization to Accounts Outside the Current Organization
- Preventing IAM Users and Agencies from Making Certain Changes
- Preventing IAM Users and Agencies from Making Specified Changes,
 Except for Specified Accounts
- Preventing IAM Users and Agencies from Making Specified Changes, Except for Specified Agencies
- Using NotResource to Prevent Starting All ECS Instances, Except for Specified Ones

Preventing Member Accounts from Leaving an Organization

```
The following SCP prevents member accounts from leaving an organization.

{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
    }
```

```
"Action": [
    "organizations:organizations:leave"
],
    "Resource": [
    "*"
    ]
}
```

Blocking Service Access for the Root User

The following SCP blocks access to the specified actions for the root user in a member account. If you want to restrict access in specific ways, you can modify the Action and Resource elements.

```
{
  "Version": "5.0",
  "Statement": [
    {
        "Effect": "Deny",
        "Action": [
            "ecs:*:"
        ],
        "Resource": [
            "*"
        ],
        "Condition": {
            "BoollfExists": {
            "g:PrincipallsRootUser": "true"
        }
     }
    }
}
```

Prohibiting Creation of Resources with Specified Tags

The following SCP prevents users from creating resource shares with the {"team": "engineering"} tag. If you want to prevent resource creation in specific ways, you can modify the Action, Resource, and Condition elements.

Prohibiting Access to Specified Regions

The following SCP prevents users from accessing all ECS resources in **regionid1** but not in any other regions. If you want to restrict access in specific ways, you can modify the Action, Resource, and Condition elements.

This SCP applies only to region-specific services. **regionid1** in the SCP is only an example for you reference. Enter the specific region ID you want when using this SCP.

Preventing Sharing with Accounts Outside an Organization

The following SCP prevents accounts within an organization from sharing resources with accounts outside the organization. You are advised to attach this SCP to the root OU of the organization so that the SCP will be applied to the entire organization.

```
{
    "Version": "5.0",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": [
        "ram:resourceShares:create",
        "ram:resourceShares:associate"

    ],
        "Resource": [
        "**"
    ],
        "Condition": {
        "ForAnyValue:StringNotLike": {
            "ram:TargetOrgPaths": [
            "organization_id/root_id/ou_id" [Note: Enter the path ID of the organization.]
        ]
        }
    }
    }
}
```

Preventing Sharing Specified Resource Types

The following SCP prevents accounts from sharing VPC subnets. You can modify the resource type in the Condition element of the SCP statement as required.

```
{
  "Version": "5.0",
  "Statement": [
  {
    "Effect": "Deny",
    "Action": [
    "ram:resourceShares:create"
  ],
    "Resource": [
```

```
],
   "Condition": {
    "ForAnyValue:StringEquals": {
        "ram:RequestedResourceType": [
            "vpc:subnet" [Note: You can change the resource type as required.]
        ]
      }
    }
}
```

Preventing Aggregation Authorization to Accounts Outside the Current Organization

The following SCP prevents accounts within an organization from granting aggregation authorization to accounts outside the organization. You are advised to attach this SCP to the root OU of your organization to prevent accounts outside your organization from collecting information about the resources of accounts in your organization. You can also attach this SCP to source accounts to prevent them from accepting authorization requests from the aggregator account.

Preventing IAM Users and Agencies from Making Certain Changes

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization.

```
{
  "Version": "5.0",
  "Statement": [
    {
        "Effect": "Deny",
        "Action": [
            "ram:resourceShares:update",
            "ram:resourceShares:delete",
            "ram:resourceShares:associate",
            "ram:resourceShares:disassociate",
            "ram:resourceShares:disassociatePermission",
            "ram:resourceShares:disassociatePermission"
            ],
            "Resource": [
            "ram:*:resourceShare:resource-id"
            ]
```

```
}
1
}
```

Preventing IAM Users and Agencies from Making Specified Changes, Except for Specified Accounts

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization, except for specified accounts.

```
"Version": "5.0",
"Statement": [
  "Effect": "Deny",
  "Action": [
   "ram:resourceShares:update",
    "ram:resourceShares:delete",
   "ram:resourceShares:associate",
   "ram:resourceShares:disassociate",
    "ram:resourceShares:associatePermission",
    "ram:resourceShares:disassociatePermission"
  "Resource": [
   "ram::*:resourceShare:resource-id"
  "Condition": {
    "StringNotEquals": {
     "g:DomainId": [
      "account-id" [Note: Enter the ID of the account to deny.]
```

Preventing IAM Users and Agencies from Making Specified Changes, Except for Specified Agencies

The following SCP prevents IAM users and agencies from making changes to resource shares created in all accounts in your organization, except for specified agencies.

```
{
  "Version": "5.0",
  "Statement": [
    {
        "Effect": "Deny",
        "Action": [
            "ram:resourceShares:create"
        ],
        "Resource": [
            "**"
        ],
        "Condition": {
            "StringNotMatch": {
                "g:PrincipalUrn": "sts::*:assumed-agency:AgencyName/*"
        }
     }
     }
}
```

Using NotResource to Prevent Starting All ECS Instances, Except for Specified Ones

The following SCP uses NotResource to prevent starting all ECS instances, except for ecs:*:8c1eef3a241xxxxxxxxx3a6b0252e783:instance:test-ecs.

5.7 System-defined SCPs

The following table lists the SCPs preconfigured on Huawei Cloud.

Table 5-2 Huawei Cloud SCPs

Policy	Description
FullAccess	Allows all permissions on all resources.

Ⅲ NOTE

At least one SCP must be attached to each root, OU, and account.

5.8 Cloud Services for Using SCPs

SCPs are available for the following cloud services:

Ⅲ NOTE

Cloud services for using SCPs also support IAM identity policies.

Compute

No.	Service Name	Reference
1	Elastic Cloud Server (ECS)	Elastic Cloud Server (ECS)
2	Bare Metal Server (BMS)	Bare Metal Server (BMS)
3	Image Management Service (IMS)	Image Management Service (IMS)
4	Auto Scaling (AS)	Auto Scaling (AS)

No.	Service Name	Reference
5	FunctionGraph	FunctionGraph

Storage

No.	Service Name	Reference
1	Cloud Backup and Recovery (CBR)	Cloud Backup and Recovery (CBR)
2	Elastic Volume Service (EVS)	Elastic Volume Service (EVS)
3	Scalable File Service Turbo (SFS Turbo)	Scalable File Service Turbo (SFS Turbo)
4	Object Storage Service (OBS)	Object Storage Service (OBS)

Networking

No.	Service Name	Reference
1	Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC)
2	Elastic IP (EIP)	Elastic IP (EIP)
3	NAT Gateway	NAT Gateway
4	Elastic Load Balance (ELB)	Elastic Load Balance (ELB)
5	VPC Endpoint (VPCEP)	VPC Endpoint (VPCEP)
6	Direct Connect	Direct Connect
7	Enterprise Router	Enterprise Router
8	Global Accelerator	Global Accelerator
9	Cloud Connect	Cloud Connect (CC)
10	Domain Name Service (DNS)	Domain Name Service (DNS)

Containers

No.	Service Name	Reference
1	Cloud Container Engine (CCE)	Cloud Container Engine (CCE)
2	SoftWare Repository for Container (SWR)	SWR Basic Edition

Content Delivery & Edge Computing

No.	Service Name	Reference
1	Content Delivery Network (CDN)	Content Delivery Network (CDN)

Databases

No.	Service Name	Reference
1	Relational Database Service (RDS)	Relational Database Service (RDS)
2	Document Database Service (DDS)	Document Database Service (DDS)
3	GaussDB	GaussDB
4	Data Admin Service (DAS)	Data Admin Service (DAS)

Security & Compliance

No.	Service Name	Reference
1	Cloud Native Anti-DDoS Basic	Cloud Native Anti-DDoS Basic
2	Cloud Native Anti-DDoS Advanced (CNAD)	Cloud Native Anti-DDoS Advanced (CNAD)
3	Advanced Anti-DDoS (AAD)	Advanced Anti-DDoS (AAD)
4	Data Encryption Workshop (DEW) contains the following microservices:	Data Encryption Workshop (DEW)
	 Key Management Service (KMS) 	
	 Cloud Secret Management Service (CSMS) 	
	Key Pair Service (KPS)	
	Dedicated Hardware Security Module (Dedicated HSM)	
5	Host Security Service (HSS)	Host Security Service (HSS)
6	SecMaster	SecMaster
7	Cloud Firewall (CFW)	Cloud Firewall (CFW)
8	Data Security Center (DSC)	Data Security Center (DSC)
9	Cloud Bastion Host (CBH)	Cloud Bastion Host (CBH)
10	Database Security Service (DBSS)	Database Security Service (DBSS)

No.	Service Name	Reference
11	Web Application Firewall (WAF)	Web Application Firewall (WAF)

ΑI

No.	Service Name	Reference
1	ModelArts	ModelArts

Analytics

No.	Service Name	Reference
1	Data Lake Insight (DLI)	Data Lake Insight (DLI)
2	DataArts Studio	DataArts Studio
3	Cloud Search Service (CSS)	Cloud Search Service (CSS)

Middleware

No.	Service Name	Reference
1	Distributed Cache Service (DCS)	Distributed Cache Service (DCS)
2	Distributed Message Service for Kafka	Distributed Message Service for Kafka
3	Distributed Message Service for RabbitMQ	Distributed Message Service for RabbitMQ
4	Distributed Message Service for RocketMQ	Distributed Message Service for RocketMQ
5	Cloud Service Engine (CSE)	Cloud Service Engine (CSE)
6	API Gateway	API Gateway

Developer Services

No.	Service Name	Reference
1	CodeArts	CodeArts
2	CodeArts Pipeline	CodeArts Pipeline
3	Cloud Application Engine (CAE)	Cloud Application Engine (CAE)

Video

No.	Service Name	Reference
1	Live	Live

Management & Governance

No.	No. Service Name Reference		
1	Simple Message Notification (SMN)	Simple Message Notification (SMN)	
2	Log Tank Service (LTS)	Log Tank Service (LTS)	
3	3 Identity and Access Management (IAM) Identity and Access Management (IAM)		
4	IAM Identity Center	IAM Identity Center	
5	Organizations	Organizations	
6	Resource Access Manager (RAM)	Resource Access Manager (RAM)	
7	Enterprise Project Management Service (EPS)		
8	Tag Management Service (TMS)	Tag Management Service (TMS)	
9	Config (original service name: Config RMS)		
10	IAM Access Analyzer	IAM Access Analyzer	
11	Cloud Trace Service (CTS)	Cloud Trace Service (CTS)	
12	Application Operations Management (AOM)	Application Operations Management (AOM)	
13	Application Performance Management (APM)	Application Performance Management (APM)	
14	Optimization Advisor (OA)	Optimization Advisor (OA)	

Migration

No.	Service Name	Reference
1	Object Storage Migration Service (OMS)	Object Storage Migration Service (OMS)

No.	Service Name	Reference
2	Server Migration Service (SMS)	Server Migration Service (SMS)

User Support

No.	Service Name	Reference
1	Billing Center	Billing Center
2	Cost Center	Cost Center
3	My Account	My Account
4	Enterprise Center	Enterprise Center

5.9 Regions for Using SCPs

SCPs are available in the following regions:

□ NOTE

Regions for using SCPs also support the use of IAM identity policies.

Table 5-3 Regions for using SCPs

Region Name	Region Code
AP-Singapore	ap-southeast-3
AP-Bangkok	ap-southeast-2
AP-Jakarta	ap-southeast-4
AP-Manila	ap-southeast-5
CN East-Shanghai1	cn-east-3
CN East-Shanghai2	cn-east-2
CN-Hong Kong	ap-southeast-1
CN North-Beijing1	cn-north-1
CN North-Beijing4	cn-north-4
CN South-Guangzhou	cn-south-1
CN North-Ulanqab1	cn-north-9
CN Southwest-Guiyang1	cn-southwest-2
CN East-Qingdao	cn-east-5

Region Name	Region Code
TR-Istanbul	tr-west-1
AF-Johannesburg	af-south-1
LA-Mexico City1	na-mexico-1
LA-Mexico City2	la-north-2
LA-Sao Paulo1	sa-brazil-1
LA-Santiago	la-south-2
ME-Riyadh	me-east-1
AF-Cairo	af-north-1
CN East2	cn-east-4
CN North3	cn-north-12

6 Managing Tag Policies

6.1 Overview of a Tag Policy

Introduction

Tag policies are a type of policy that can help you standardize tags across resources in your organization's accounts. In a tag policy, you specify tagging rules applicable to resources when they are tagged. Untagged resources and tags that are not defined in the tag policy are not evaluated for compliance with the tag policy.

For example, a tag policy can specify that a tag attached to a resource must use the case treatment and tag values defined in the tag policy. If the case and value of the tag do not comply with the tag policy, the resource will be marked as noncompliant.

Currently, tag policies can be used as preventive governance policies. Specifically, if enforcement is enabled for a tag policy, non-compliant tagging operations will be prevented from being performed on specified resource types.

You can attach tag policies to the root OU, other OUs, and accounts within your organization. When you attach a tag policy to the root OU and other OUs, all their child OUs and member accounts inherit that tag policy. The effective tag policy for an account specifies the tagging rules that apply to the account. It is the combination of tag policies that account inherits and tag policies directly attached to that account.

Functions

Managing tag policies

You can create, update, delete, attach, or detach tag policies. OUs and accounts inherit tag policies from one or more of their parent nodes (such as parent OUs). The inherited tag policies are aggregated with those directly attached to the OUs and accounts to form the effective tag policy.

6.2 Tag Policy Syntax

Basic Syntax

The following tag policy shows basic tag policy syntax:

```
"tags": {
   "costcenter": {
                              <!-- policy key -->
      "tag_key": {
         '@@assign": "CostCenter"
                                                <!-- tag key -->
      "tag_value": {
         '@@assign": [
           "100".
                              <!-- policy value -->
           "200"
        ]
      "enforced_for": {
                                   <!-- enforcement -->
         '@@assign": [
           "apig:instance"
                                       <!-- service or resource type -->
     }
  }
}
```

- Policy key: A policy key uniquely identifies a policy statement. It must match the value for the tag key, except for the case treatment.
- Tag key: The value for the tag key must match the value for the policy key. But since the policy key value is case insensitive, the capitalization can be different. If the tag key is not defined, lowercase is the default case treatment for tag keys. In this example, **costcenter** is the policy key and **CostCenter** is the tag key, and **CostCenter** is the case treatment that is required for compliance with the tag policy. If the policy key is set to **CostCenter** and the tag key is not defined, the lowercase **costcenter** will be the case treatment required for tag compliance evaluation.
- Policy value: A list of one or more acceptable tag values for the tag key. If you
 do not specify tag values for a tag key, any value (including no value at all) is
 considered compliant.
- Enforcement: An enforced_for field indicates whether to prevent any noncompliant tagging operations on specified services and resources. If you do not specify any services or resource types in a tag policy, the tag policy will not apply to any resources.
- Wildcard: You can use the wildcard (*) in tag values and the **enforced_for** field provided that you adhere to the following rules:
 - You can use only one wildcard for each tag value. For example,
 *@example.com is allowed, but *@*.com is not.
 - For the enforced_for field, you can use <service>:* to enable enforcement for all resources for a service, but you cannot use a wildcard to specify all services or specify a resource of all services.

Inheritance Operators

In the preceding example tag policy, the operator @@assign used in the tag key, tag value, and enforcement is an inheritance operator.

Inheritance operators specify how directly attached tag policies and inherited tag policies are merged into the account's effective tag policy. Such operators include value-setting operators and child control operators.

Value-setting operators

You can use the following value-setting operators to control how your policy interacts with its parent policies.

Table 6-1 Value-setting operators

Operator	Description
@@assign	Overwrites any inherited policy settings with the specified setting. If the specified setting is not inherited, this operator adds it to the effective tag policy. This operator can apply to any policy setting of any type.
	For single-valued settings, this operator replaces the inherited value with the specified value.
	For multi-valued settings (JSON arrays), this operator removes all inherited values and replaces them with the values specified for this policy.
@@append	Adds the specified settings to the inherited settings, without deleting any settings. If the specified setting is not inherited, this operator adds it to the effective tag policy. You can only use this operator with multi-valued settings.
	This operator adds the specified value to any values in the inherited array.
@@remove	Removes the specified inherited setting (if there is one) from the effective policy. You can only use this operator with multi-valued settings.
	This operator removes only the specified values from the array of values inherited from the parent policies. Other values can be retained in the array and inherited by child policies.

Child control operators

Child control operators specify which value-setting operators child OUs and accounts can use in child policies. By default, all operators (@@all) are allowed.

- "@@operators_allowed_for_child_policies":["@@all"] indicates that child OUs and accounts can use any operator in policies. By default, all operators are allowed in child policies.
- "@@operators_allowed_for_child_policies":["@@assign", "@@append",
 "@@remove"] indicates that child OUs and accounts can use only the

- specified operators in child policies. You can specify one or more valuesetting operators in this child control operator.
- "@@operators_allowed_for_child_policies":["@@none"] indicates that child OUs and accounts cannot use operators in policies. You can use this operator to effectively lock the values defined in a parent policy so that the child policies cannot add, append, or delete those values.

6.3 Enabling or Disabling the Tag Policy Type

You can enable or disable the tag policy type from the organization' management account, but not from any delegated administrator.

Enabling the Tag Policy Type

Before you can create and attach tag policies to the OUs and accounts in your organization, you must enable the tag policy type. The only way to enable the tag policy type is by using the organization's management account.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Enable** in the **Operation** column of tag policies.

Figure 6-1 Enabling the tag policy type



Step 3 In the displayed dialog box, select the check box and click **OK**.

----End

Disabling the Tag Policy Type

If you no longer want to use tag policies in your organization, you can disable the tag policy type only from the organization's management account.



- After the tag policy type is disabled in an organization, all tag policies are automatically detached from all OUs and accounts in the organization. However, the policies are not deleted.
- If you disable the tag policy type, attachments of tag policies to entities will be lost. If you later re-enable the tag policy type, you must use the management account to re-attach tag policies to the entities.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Disable** in the **Operation** column of tag policies.

Figure 6-2 Disabling the tag policy type



Step 3 Click **OK** in the displayed dialog box.

----End

6.4 Creating a Tag Policy

To standardize the usage of tags in your organization, you can create a tag policy to formulate tag rules.

You can create a tag policy from the organization administrator, but not from any delegated administrator.

Procedure

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** Access the **Policies** page, and click **Tag policies**.

Figure 6-3 Accessing the Tag policies page



- **Step 3** Click **Create Policy**.
- **Step 4** Edit the policy name. The policy name is automatically generated when you create a policy, but you can change the policy name if needed. Ensure that you are entering a unique policy name. It must be different from any other existing policy.

(Optional) You can also enter a description for the policy.

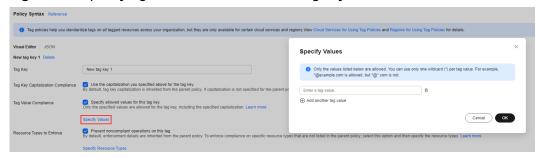
- **Step 5** Edit the policy content. Currently, you can edit the policy content using the visual editor or JSON.
 - Visual editor: When you use the visual editor to edit a policy, you do not need to understand the JSON syntax. After you edit in the visual editor, the new policy is generated automatically. The procedure is as follows:
 - a. Enter the key for the tag you want to define in the tag policy.
 - b. Use the capitalization you specified above for the tag key.

If you select this option, the capitalization you specified for **Tag Key** is used for checking compliance. If you do not select this option, tag keys in all lowercase characters are considered compliant even if **Tag Key** contains uppercase characters. For example, when you enter **CostCenter** for **Tag Key**, if you select this option, **CostCenter** will be the standard for compliance check; if you do not select this option, **costcenter** will be the standard.

c. Specify allowed values for this tag key.

If you select this option and click **Specify Values** to specify one or more allowed values for the tag key, only those values you specified are considered compliant. If you do not select this option or you select this option but do not specify any values, any value (including no value at all) is considered compliant.

Figure 6-4 Specifying allowed values for this tag key



d. Specify resource types to enforce the tag policy.

Select the **Prevent noncompliant operations on this tag.** option and click **Specify Resource Types**. In the displayed dialog box, read and confirm the effects of using tag policies. Then, select resource types and click **OK**.

∩ NOTE

If you do not specify any services or resource types, the tag policy will not apply to any resources.

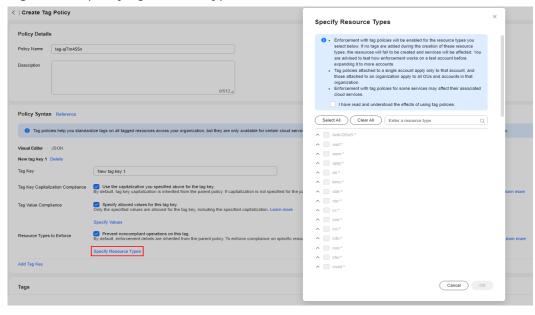


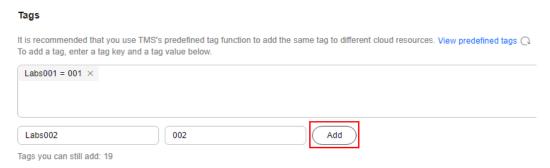
Figure 6-5 Specifying resource types

- e. Click Add Tag Key to add another tag key to this tag policy.
- JSON: When using JSON syntax, you can edit the policy text by referring to **Tag Policy Syntax**. The system automatically verifies the syntax. If the syntax is incorrect, modify it as prompted.

Figure 6-6 Editing a policy using JSON

Step 6 (Optional) Add one or more tags. Enter a tag key and a tag value, and click **Add**.

Figure 6-7 Adding a tag



Step 7 Click **Save** in the lower right corner. If the tag policy is created successfully, it will be added to the list.

----End

6.5 Viewing the Effective Tag Policy

You can attach tag policies to the root OU, other OUs, and accounts within your organization. When you attach a tag policy to the root OU and other OUs, all their child OUs and member accounts inherit that tag policy. The effective tag policy for an account specifies the tagging rules that apply to the account. It is the combination of tag policies that account inherits and tag policies directly attached to that account.

The following describes how a tag policy is prioritized as the effective tag policy:

- Tag policies attached to entities at the same hierarchy level:
 - Single-valued operators: If you attach multiple tag policies, the first policy using the @@assign operator will be considered to be the effective tag policy.
 - Multi-valued operators: If you attach multiple tag policies, the first policy using the @@assign operator will be considered to be the effective tag policy, and the @@append and @@remove operators used by other policies still take effect.
- Tag policies attached to entities at the different hierarchy levels:
 If the upper- and lower-level entities use the same tag key, tag policies are calculated from the upper-level entities to the lower-level entities based on the types of child control operators to comprise the effective tag policy. If the upper and lower levels use different tag keys, the combination of their tag policies comprises the effective tag policy.

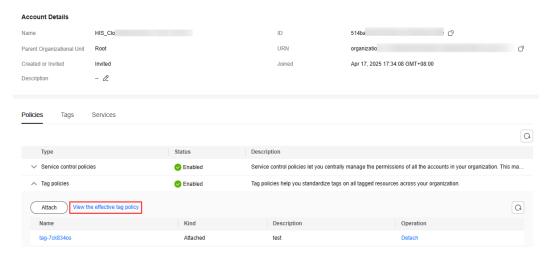
To view the effective tag policy for the root OU, other OUs, and accounts of an organization on the management console, use the following procedure:

Procedure

- **Step 1** Go to the Organizations console and access the **Organization** page.
- **Step 2** Click the root OU, specific OU, or account of your organization. You can view its details on the right of the organization tree.

- Step 3 Click the Policies tab.
- **Step 4** Expand the tag policy list and click **View the effective tag policy** above the list. The effective tag policy is presented in JSON.

Figure 6-8 Viewing the effective tag policy



6.6 Editing or Deleting a Tag Policy

The following describes how to edit and delete a tag policy.

You can edit or delete a tag policy from the organization administrator, but not from a delegated administrator.

Editing a Tag Policy

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- Step 2 Access the Policies page, and click Tag policies.
- **Step 3** Locate the target tag policy and click **Modify** in the **Operation** column. The **Edit Tag Policy** page is displayed.

Figure 6-9 Editing a tag policy



- **Step 4** Enter a new policy name and description.
- **Step 5** Edit the policy content if needed. You can choose either visual editor or JSON to edit the policy.

Step 6 Click **Save** in the lower right corner. If the tag policy is updated successfully, it will be added to the list.

----End

Deleting a Tag Policy

A tag policy that is attached to OUs or accounts cannot be deleted. To delete such a tag policy, you need to detach it from the OUs or accounts first.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** Access the **Policies** page, and click **Tag policies**.
- **Step 3** Locate the tag policy you want to delete and click **Delete** in the **Operation** column.
- **Step 4** Click **OK** in the displayed dialog box.

Figure 6-10 Deleting a tag policy



----End

6.7 Attaching or Detaching a Tag Policy

You can attach a tag policy to or detach it from the root OU, other OUs or accounts from the organization's management account.

Constraints

- You can attach up to 10 tag policies to an account.
- You can attach or detach a tag policy from only the organization administrator, but not from a delegated administrator.
- Tag policies are applied within 30 minutes after they are attached.

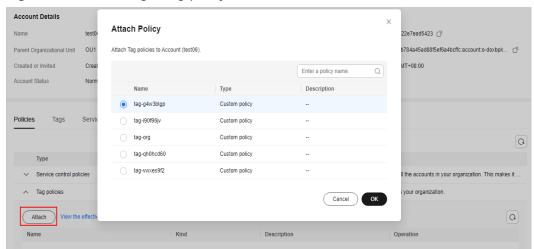
Attaching a Tag Policy

Method 1:

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU or account you want to attach a tag policy to.
- **Step 3** On the details page, click the **Policies** tab. On the page, expand **Tag policies** and click **Attach**.

Step 4 Select the tag policy you want to attach and click **OK**.

Figure 6-11 Attaching a tag policy



----End

Method 2:

- Step 1 On the Organizations console, access the Policies page.
- **Step 2** Click **Tag policies**. The list of tag policies is displayed.
- **Step 3** Locate the tag policy you want to attach and click **Attach** in the **Operation** column. Then, select the OU or account you want to attach the policy to.
- Step 4 Click OK.

Figure 6-12 Attaching a tag policy



----End

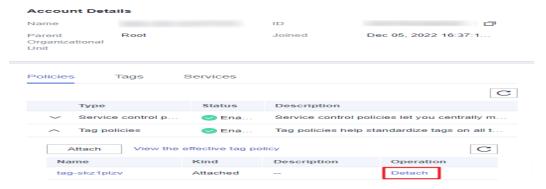
Detaching a Tag Policy

Method 1:

Step 1 Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.

- **Step 2** Select the OU or account you want to detach a tag policy from.
- **Step 3** On the details page, click the **Policies** tab. On the page, expand **Tag policies**, locate the target tag policy and click **Detach** in the **Operation** column.

Figure 6-13 Detaching a tag policy



- **Step 4** Click **Detach** in the displayed dialog box.
 - ----End

Method 2:

- **Step 1** On the Organizations console, access the **Policies** page.
- **Step 2** Click **Tag policies**. The list of tag policies is displayed.
- **Step 3** Click the name of the target tag policy and click the **Targets** tab.
- **Step 4** Locate the OU or account that you want to detach the tag policy from and click **Detach** in the **Operation** column.
- Step 5 Click OK.

Figure 6-14 Detaching a tag policy



----End

6.8 Cloud Services for Using Tag Policies

Tag policies are available for the following cloud services and resource types:

Table 6-2 Supported cloud services and resources types

Service Name	Resource Type
Cloud Native Anti-DDoS Basic	Public IP addresses
Anti-DDoS Service	Instances
Application Operations Management (AOM)	Alarm rules
API Gateway	Instances
Auto Scaling (AS)	Scaling groups
Bare Metal Server (BMS)	Instances
Cloud Bastion Host (CBH)	Instances
Cloud Backup and Recovery (CBR)	Vaults
Cloud Connect	Bandwidth packagesCentral networkCloud connections
Cloud Container Engine (CCE)	Clusters
Cloud Container Instance (CCI)	Namespace
Content Delivery Network (CDN)	Domain
Cloud Eye	Alarm rules
Cloud Firewall (CFW)	Instances
Cloud Native Anti-DDoS Advanced (CNAD)	Packages
Cloud Service Engine (CSE)	Engine
Cloud Secret Management Service (CSMS)	Secret
Cloud Search Service (CSS)	ClustersLog streamRepository
Cloud Trace Service (CTS)	Trackers
DataArts Studio	InstancesWorkspace
Database Security Service (DBSS)	Audit instances

Service Name	Resource Type
Direct Connect	 Direct connections Global DC gateways Lag Virtual gateways Virtual interfaces
Distributed Cache Service (DCS)	Instances
Document Database Service (DDS)	Instance names
Dedicated Hardware Security Module (Dedicated HSM)	Hardware security modules
Data Lake Insight (DLI)	 Databases Enhanced datasource connections Elastic resource pools Jobs Queues Resources
Distributed Message Service (DMS)	Kafka instancesRabbitMQ instancesRocketMQ instances
Domain Name Service (DNS)	PTRDomain names
Data Replication Service (DRS)	Jobs
Data Warehouse Service (DWS)	Clusters
Elastic Cloud Server (ECS)	Instances
Elastic Load Balance (ELB)	ListenersLoad balancers
Enterprise Router	AttachmentsInstancesRoute tables
Elastic Volume Service (EVS)	Volume
FunctionGraph	Functions
Global Accelerator (GA)	AcceleratorsListeners
GaussDB	Instances
GaussDB(for MySQL)	Instances

Service Name	Resource Type
GeminiDB (originally named GaussDB for NoSQL)	Instances
Identity and Access Management (IAM)	AgenciesUsers
Image Management Service (IMS)	Images
IoT Device Access (IoTDA)	Instances
Key Management Service (KMS)	Customer master keys
Log Tank Service (LTS)	Log access configurationHost groupsLog groupsLog stream
ModelArts	NotebookResource poolsServicesTraining jobs
MapReduce Service (MRS)	Clusters
NAT Gateway	Public gatewaysPrivate gatewaysPrivate transit IP addressesTransit subnets
Object Storage Service (OBS)	Buckets
Organizations	AccountsOrganizational unitsPoliciesRoot
Private Certificate Authority (PCA)	Private CA
Resource Access Manager (RAM)	Resource shares
Relational Database Service (RDS)	Instances
Config (original service name: RMS)	Policy assignments
SSL Certificate Manager (SCM)	Certificates
SecMaster	Workspace
ServiceStage	ApplicationsEnvironment

Service Name	Resource Type
Scalable File Service Turbo (SFS Turbo)	SFS Turbo (shares)
Simple Message Notification (SMN)	Topics
Virtual Private Cloud (VPC)	 Public IP addresses Subnets VPC Network ACLs (firewalls) Security groups
VPC Endpoint (VPCEP)	Endpoint servicesEndpoints
Virtual Private Network (VPN)	Peer gatewaysVPN connectionsVPN gateways
Web Application Firewall (WAF)	Premium instances

6.9 Regions for Using Tag Policies

Tag policies are available in the following regions:

Table 6-3 Supported regions

Region Name	Region Code
AP-Singapore	ap-southeast-3
AP-Bangkok	ap-southeast-2
AP-Jakarta	ap-southeast-4
CN East-Shanghai1	cn-east-3
CN East-Shanghai2	cn-east-2
CN-Hong Kong	ap-southeast-1
CN North-Beijing1	cn-north-1
CN North-Beijing4	cn-north-4
CN South-Guangzhou	cn-south-1
CN North-Ulanqab1	cn-north-9
CN Southwest-Guiyang1	cn-southwest-2
CN East-Qingdao	cn-east-5

Region Name	Region Code
TR-Istanbul	tr-west-1
AF-Johannesburg	af-south-1
LA-Mexico City1	na-mexico-1
LA-Mexico City2	la-north-2
LA-Sao Paulo1	sa-brazil-1
LA-Santiago	la-south-2
ME-Riyadh	me-east-1

Managing Trusted Services

7.1 Overview of a Trusted Service

What Is a Trusted Service?

You can use the management account in Organizations to enable trusted access for a supported Huawei Cloud service, called a trusted service. A trusted service can perform tasks in your organization on your behalf. Each trusted service has access to the information about the OUs and member accounts in your organization and also can manage the entire organization. For example, if you enable CTS as a trusted service for Organizations, CTS can obtain information about OUs and member accounts to record the operations in all accounts within the organization. For cloud services that can be enabled with trusted access, see Trusted Services for Organizations.

Delegated Administrator

A delegated administrator account is a member account that has special permissions in an organization. The management account of your organization can designate a member account to be a delegated administrator account for a trusted service. All the users in the delegated administrator account will have organizational management capabilities. For example, if a member account becomes the delegated administrator of CTS, the account can view the CTS logs of all member accounts in the organization.

Service-linked Agency

The Organizations service uses IAM trust agencies to enable trusted services to perform tasks on your behalf in your organization's member accounts. When you enable a trusted service, the service can request that Organizations create a service-linked agency in its member accounts. The trusted service does this asynchronously, as needed. The service-linked agency has predefined IAM permissions that allow the trusted service to perform specific tasks within that account. This means that the capabilities of that cloud service are extended to the entire multi-account organization. For details about the supported trusted services and their functions, see **Trusted Services for Organizations**.

When you create an account in your organization or invite an existing account to join your organization, Organizations provisions the member account with a service-linked agency with the system-defined permission **OrganizationsServiceLinkedAgencyPolicy**, which is applicable to all resources. Only the Organizations service itself can assume this agency. This agency has permission that allows Organizations to create service-linked agencies for other cloud services.

Organizations SCPs do not affect service-linked agencies, and operations performed using service-linked agencies are not restricted by SCPs.

7.2 Enabling or Disabling a Trusted Service

- If the organization administrator disables trusted access for a cloud service, the service can no longer create a service-linked agency in the member accounts.
- If the organization administrator closes the organization or a member account leaves the organization, Organizations will clear its service-linked agency.
- Before disabling trusted access for the AOM service, delete multi-account instances on the AOM console and then disable the trusted access on the Organizations console. Otherwise, the multi-account instances will continue retrieving the member accounts' metric data.
- Before disabling trusted access for the LTS service, delete the configurations of multi-account log aggregation on the LTS console and then disable the trusted access on the Organizations console. Otherwise, the multi-account log aggregation will continue retrieving the member accounts' logs.

Enabling a Trusted Service

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Services** page, locate the target trusted service and click **Enable Access** in the **Operation** column.
- **Step 3** Click **OK** in the displayed dialog box.

Organizations

Organization

Accounts
Policies

Service
Services

Application Operations Management (AOM)
Cloud Backup and Recovery (CBR)
Cloud Backup and Recovery (CBR)
Cloud Eyer (CES)
Cloud Eyer (CES)
Cloud Fire/Vall (CPV)
Access dasabled

Cloud Fire/Vall (CPV)
Access dasabled

Cloud Trace Service (CTS)
Access dasabled

Cloud Trace Service (CTS)
Access dasabled

Access dasabled

Access dasabled

Access Specify Delegated Administrator View Delegated Administrator View

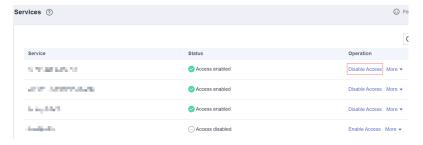
Figure 7-1 Enabling a trusted service

Disabling a Trusted Service

When logging in as the organization's management account, you can disable trusted services.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Services** page, locate the target trusted service and click **Disable Access** in the **Operation** column.

Figure 7-2 Disabling a trusted service



Step 3 In the displayed dialog box, enter "Confirm" and click **OK**.

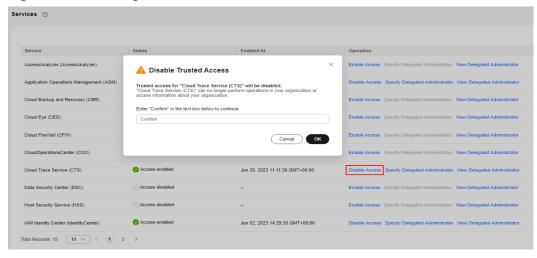


Figure 7-3 Disabling a trusted service

7.3 Trusted Services for Organizations

Log in to the Organizations console as an organization administrator or using the management account and access the **Services** page to view the trusted service list.

The following table lists the cloud services that can be used with Huawei Cloud Organizations.

Table 7-1 Trusted services for Organizations

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Config	You can create compliance rules, conformance packages, and resource aggregators for a given organization. The organization administrator or the delegated Config administrator can perform unified configurations, which will be applied to all normal member accounts in the organization.	Supported	Unlimited	 Organizati on Rules Organizati on Conforman ce Packages Resource Aggregatio n

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Resource Access Manager (RAM)	You can easily share resources within a given organization. When your account is managed by an organization, you can share resources with all accounts in the organization. Accounts in the same organization can use the shared resources without being invited.	Supported	Unlimited	Enabling Sharing with Organizations
Cloud Trace Service (CTS)	You can configure an organization tracker for a given organization. The organization administrator or delegated CTS administrator can apply the organization tracker to the entire organization for cloud audit, such as multi-account security audit.	Supported	Unlimited	Organization Trackers

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Application Operations Management (AOM)	You can create Prometheus instances of the multi-account aggregation type. With this function enabled for a given organization, the organization administrator or delegated AOM administrator can centrally monitor the cloud service metrics across multiple member accounts in the organization.	Supported	Unlimited	Prometheus for Multi- Account Aggregation

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Cloud Backup and Recovery (CBR)	You can manage backup and replication policies for a given organization. The organization administrator or delegated CBR administrator can centrally create and configure organizational backup policies and replication policies for member accounts in the organization.	Supported	Unlimited	Organization Policy Management
Cloud Eye	You can view the dashboards across accounts in a given organization. The organization administrator or delegated Cloud Eye administrator can view the dashboards of all accounts in the organization.	Supported	Unlimited	Viewing Dashboards Across Accounts

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Cloud Firewall (CFW)	You can securely and reliably aggregate data from and access resources across accounts. The organization administrator or delegated CFW administrator can protect the EIPs of all member accounts in the organization in a unified manner.	Supported	Unlimited	Multi-Account Management
Data Security Center (DSC)	You can securely and reliably aggregate data from and access resources across accounts. The organization administrator and delegated DSC administrator can protect the data security of all member accounts in the organization, without login using each account.	Supported	Unlimited	Multi-Account Management

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Host Security Service (HSS)	You can securely and reliably aggregate data from and access resources across accounts. The organization administrator or delegated HSS administrator can protect the workloads of all member accounts in the organization in a unified manner.	Supported	Unlimited	Account Management
IAM Identity Center	You can use IAM Identity Center to centrally manage your workforce identities and their access to multiple accounts in your organization. You can create identities for your entire enterprise at one go and give them single sign-on (SSO) access with managed permissions.	Supported	Unlimited	What Is IAM Identity Center?

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Log Tank Service (LTS)	You can deploy a log aggregation center to aggregate logs across accounts. The organization administrator or delegated LTS administrator can copy the log streams of specified account in the organization on the LTS console to centrally store and analyze multi-account logs. This can meet the scenariospecific requirements for security compliance and centralized analysis.	Supported	Unlimited	Multi-Account Log Center

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
SecMaster	You can apply workspace agencies to multiple accounts in a given organization. The organization administrator or delegated SecMaster administrator can create a workspace agency for one or more accounts in the organization.	Supported	Unlimited	Creating an Agency
IAM Access Analyzer	Access Analyzer provides organization- wide access analysis. The organization administrator or delegated administrator can create and manage access analyzers in a given organization, for example, to identify resources in the organization that are shared with external principals.	Supported	1	None

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Cloud Operations Center (COC)	Working with cross-account management of Organizations , COC allows an organization administrator or delegated service administrator to view the O&M situation and resource status of members in the organization and also to perform operations across accounts.	Supported	1	None

Service Name	Benefits of Using with Organization s	Delegated Administrato r	Maximum Number of Delegated Administrato rs	Reference
Resource Formation Service (RFS)	RFS supports multi-account management based on Organizations . The organization administrator or delegated RFS administrator can specify an OU to orchestrate resources of multiple accounts in an organization across regions. There is no need to manually create or deploy agencies.	Supported	Unlimited	None

7.4 Specifying, Viewing, or Removing a Delegated Administrator

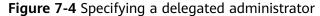
NOTICE

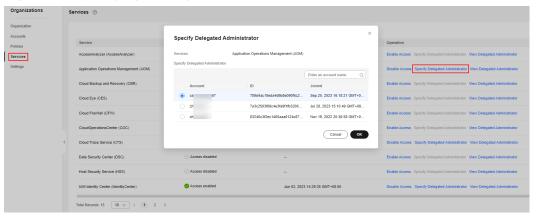
- Before removing the delegated administrator of the trusted service AOM, delete the multi-account instances on the AOM console and then access the Organizations console to start removal. Otherwise, the multi-account instances will continue retrieving the member accounts' metric data.
- Before removing the delegated administrator of the trusted service LTS, delete
 the configurations of multi-account log aggregation on the LTS console and
 then access the Organizations console to start removal. Otherwise, the multiaccount log aggregation will continue retrieving the member accounts' logs.

Specifying a Delegated Administrator

An account being closed cannot be specified as a delegated administrator.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Services** page, locate the target trusted service and click **Specify Delegated Administrator** in the **Operation** column.
- **Step 3** Select the account to be specified as the delegated administrator, and click **OK**.





----End

Viewing a Delegated Administrator

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Services** page, locate the target trusted service and click **View Delegated Administrator** in the **Operation** column.
- **Step 3** View the details about the delegated administrator of the trusted service.

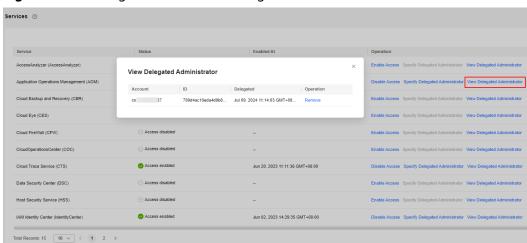
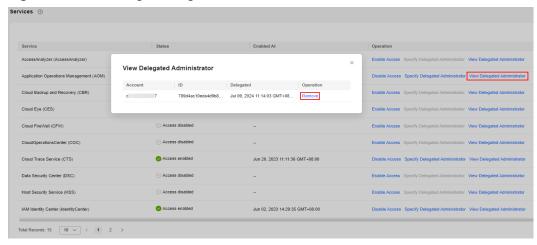


Figure 7-5 Viewing details about a delegated administrator

Removing a Delegated Administrator

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Services** page, locate the target trusted service and click **View Delegated Administrator** in the **Operation** column.
- **Step 3** In the displayed dialog box, click **Remove** in the **Operation** column.

Figure 7-6 Removing a delegated administrator



Step 4 Click **OK** in the displayed dialog box.

----End

8 Managing Tags

8.1 Overview of a Tag

Tag Introduction

A tag is a custom label you use to identify, categorize, and search for cloud resources. You can add tags to the following organization resources:

- Organization root
- Organizational units (OUs)
- Accounts
- Service control policies (SCPs)
- Tag policies

You can add tags at the following times:

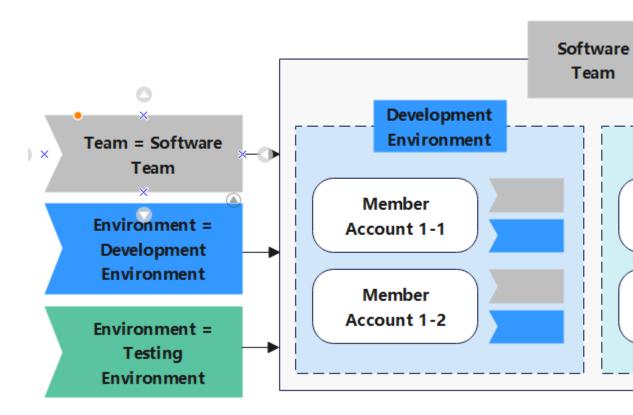
- When you create OUs, accounts, SCPs, or tag policies, you can add tags.
- When you view details about the organization root, OUs, accounts, SCPs, or tag policies, you can add, update, view, or delete tags on their details pages.

Basics of Tags

Tags help you to identify your cloud resources. When you have many cloud resources of the same type, you can use tags to classify them by dimension (for example, use, owner, or environment).

Figure 8-1 shows an example of how tags work. In this example, two tags were assigned to each member account. Each tag contains a key and a value defined by the user. The key of one tag is **Team**, and the key of another tag is **Environment**.

Figure 8-1 Example of tags



You can quickly search for and filter specific cloud resources based on the tags added to them. For example, you can define a set of tags for cloud resources in an account to track the owner and usage of each cloud resource, making resource management easier and faster.

Constraints on Using Tags

 The following basic naming and usage requirements apply to the key and value of a tag:

Tag key:

- Cannot be an empty string.
- Contains 1 to 128 characters.
- Consists of letters, digits, underscores (_), hyphens (-), and Unicode characters (\u4E00-\u9FFF).

Tag value:

- Can be an empty string.
- Contains 1 to 225 characters.
- Consists of letters, digits, underscores (_), periods (.), hyphens (-), and Unicode characters (\u4E00-\u9FFF).
- Each cloud resource can have a maximum of 20 tags.
- For each resource, each tag key must be unique and can have only one tag value.

Helpful links:

- Adding a Tag: You can add tags for your OUs, accounts, SCPs, and tag policies.
- Editing a Tag: You can update the tag keys and values for OUs, accounts, SCPs, and tag policies.
- Viewing Tag Details: You can view the tags attached to OUs, accounts, SCPs, and tag policies.
- Deleting a Tag: You can delete tags from OUs, accounts, SCPs, and tag policies.

8.2 Adding a Tag

Adding a Tag to the Root, OUs, or Accounts

Scenario

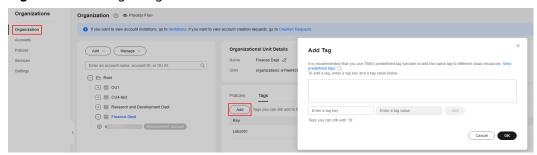
The following describes how to add a tag to the root, OUs, or accounts.

Procedure

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU to which you want to add a tag, click the **Tags** tab on the right, and click **Add**.
- **Step 3** Enter a tag key and a tag value, click **Add**, and click **OK**.

You can select a predefined tag created in TMS from the drop-down lists. For details, see Creating Predefined Tags.

Figure 8-2 Adding a tag



----End

Adding a Tag to a Policy

Scenario

The following describes how to add tags to custom SCPs and tag policies.

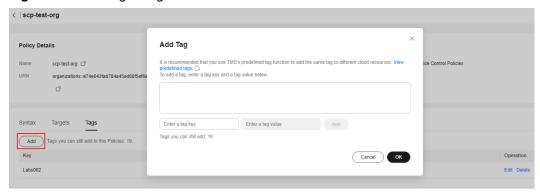
Procedure

The procedures for adding tags to custom SCPs and tag policies are similar. The following uses adding a tag to a custom SCP as an example.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Service control policies**.
- **Step 3** Click the name of a policy to go to the policy details page.
- **Step 4** Click the **Tags** tab and click **Add**.
- **Step 5** Enter a tag key and a tag value, click **Add**, and click **OK**.

You can select a predefined tag created in TMS from the drop-down lists. For details, see Creating Predefined Tags.

Figure 8-3 Adding a tag



----End

8.3 Editing a Tag

Editing a Tag for the Root, OUs, or Accounts

Scenario

The following describes how to edit a tag for the root, OUs, or accounts.

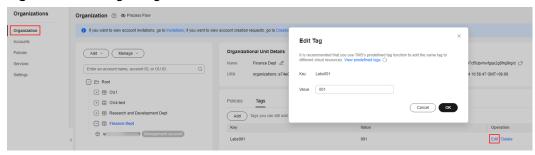
Procedure

You edit tags for the root, OUs, and accounts in the same way. The following uses editing a tag for an OU as an example.

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU for which you want to edit the tag and click the **Tags** tab in the right pane. The list of tags is displayed.

Step 3 In the displayed dialog box, enter the new tag value, and click **OK**.

Figure 8-4 Editing a tag



----End

Editing a Tag for a Policy

Scenario

The following describes how to edit tags for custom SCPs and tag policies.

Procedure

The procedures for editing tags for custom SCPs and tag policies are similar. The following uses editing a tag for a custom SCP as an example.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Service control policies**.
- **Step 3** Click the name of a policy to go to the policy details page.
- **Step 4** Click the **Tags** tab, locate the tag you want to edit, and click **Edit** in the **Operation** column.
- **Step 5** In the displayed dialog box, enter the new tag value and click **OK**.

Figure 8-5 Editing a tag



----End

8.4 Viewing Tag Details

Viewing Tag Details for the Root, OUs, or Accounts

Scenario

The following describes how to view tag details for the root, OUs, or accounts.

Procedure

You view tag details for the root, OUs, and accounts in the same way. The following uses viewing tag details of an OU as an example.

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU whose tag details you want to view and click the **Tags** tab in the pane on the right. The list of tags is displayed.
- **Step 3** View all tags attached to the OU in the tag list.

----End

Viewing Tag Details for a Policy

Scenario

The following describes how to view tag details for custom SCPs and tag policies.

Procedure

The procedures for viewing tag details for custom SCPs and tag policies are similar. The following uses viewing tag details for a custom SCP as an example.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Service control policies**.
- **Step 3** Click the name of a policy to go to the policy details page.
- **Step 4** Click the **Tags** tab to view all the tags attached to the SCP.

----End

8.5 Deleting a Tag

Deleting a Tag from the Root, OUs, or Accounts

Scenario

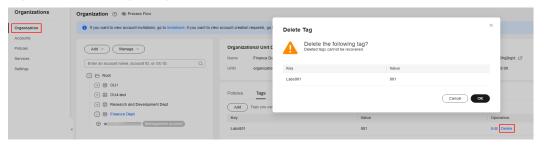
The following describes how to delete a tag from the root, OUs, or accounts.

Procedure

You delete tags from the root, OUs, and accounts in the same way. The following uses deleting a tag from an OU as an example.

- **Step 1** Log in to Huawei Cloud as the organization administrator or using the management account, navigate to the Organizations console, and access the **Organization** page.
- **Step 2** Select the OU whose tag you want to delete and click the **Tags** tab in the pane on the right.
- **Step 3** Locate the tag you want to delete and click **Delete** in the **Operation** column. Then, click **OK** in the displayed dialog box.

Figure 8-6 Deleting a tag



----End

Deleting a Tag from a Policy

Scenario

The following describes how to delete tags from custom SCPs and tag policies.

Procedure

The procedures for deleting tags from custom SCPs and tag policies are similar. The following uses deleting a tag from a custom SCP as an example.

- **Step 1** Log in to the Organizations console as an organization administrator or using the management account.
- **Step 2** On the **Policies** page, click **Service control policies**.
- **Step 3** Click the name of a policy to go to the policy details page.
- **Step 4** On the **Tags** page, locate the tag you want to delete and click **Delete** in the **Operation** column.
- **Step 5** Click **OK** in the displayed dialog box.

Figure 8-7 Deleting a tag



9 CTS Auditing

9.1 Supported Organizations Operations

With Cloud Trace Service (CTS), you can record Organizations operations for later query, auditing, and backtracking.

Table 9-1 Organizations operations that can be recorded by CTS

Operation	Resource Type	Event Name
Creating an organization	organization	createOrganization
Getting organization information	organization	showOrganization
Deleting an organization	organization	celeteOrganization
Leaving an organization	organization	leaveOrganization
Listing roots of an organization	root	listRoots
Creating an OU	organizationUnit	createOrganizationalUnit
Listing OUs	organizationUnit	listOrganizationalUnits
Getting OU information	organizationUnit	showOrganizationalUnit
Updating an OU	organizationUnit	updateOrganizationalU- nit
Deleting an OU	organizationUnit	deleteOrganizationalUnit
Inviting an account	account	inviteAccount
Creating an account	account	createAccount
Creating an account	account	createAccountV2
Closing an account	account	closeAccount

Operation	Resource Type	Event Name
Updating an account	account	updateAccount
Moving an account	account	moveAccount
Removing an account	account	removeAccount
Listing accounts in an organization	account	listAccounts
Getting account information	account	showAccount
Querying CreateAccount requests in the specified state	accountStatus	listCreateAccountStatus- es
Getting the account creation status	accountStatus	showCreateAccountSta- tus
Querying CloseAccount requests in the specified state	accountStatus	listCloseAccountStatuses
Accepting an invitation	handshake	acceptHandshake
Declining an invitation	handshake	declineHandshake
Canceling an invitation	handshake	cancelHandshake
Getting invitation information	handshake	showHandshake
Listing received invitations	handshake	listReceivedHandshakes
Listing sent invitations	handshake	listHandshakes
Enabling a trusted service	trustedService	enableTrustedService
Disabling a trusted service	trustedService	disableTrustedService
Listing trusted services	trustedService	listTrustedServices
Configuring a delegated administrator	delegatedAdministrator	registerDelegatedAdmi- nistrator
Removing a delegated administrator	delegatedAdministrator	deregisterDelegatedAd- ministrator
Listing services managed by a delegated administrator account	delegatedAdministrator	listDelegatedServices
Listing delegated administrator accounts	delegatedAdministrator	listDelegatedAdministra- tors

Operation	Resource Type	Event Name
Creating a policy	policy	createPolicy
Updating a policy	policy	updatePolicy
Deleting a policy	policy	deletePolicy
Listing policies	policy	listPolicies
Getting policy information	policy	showPolicy
Enabling a policy type	policy	enablePolicyType
Disabling a policy type	policy	disablePolicyType
Querying the dry-run configurations of an organizational policy	policy	showDryRunConfig
Updating the dry-run configurations of an organizational policy	policy	updateDryRunConfig
Creating a dry-run policy	policy	createDryRunPolicy
Listing dry-run policies	policy	listDryRunPolicies
Querying information about a dry-run policy	policy	showDryRunPolicy
Updating information about a dry-run policy	policy	updateDryRunPolicy
Deleting information about a dry-run policy	policy	deleteDryRunPolicy
Attaching a policy	policy	attachPolicy
Detaching a policy	policy	detachPolicy
Attaching a dry-run policy to an entity	policy	attachDryRunPolicy
Detaching a dry-run policy from an entity	policy	detachDryRunPolicy
Listing entities for the specified policy	policy	listEntitiesForPolicy
Listing all entities that a specified dry-run policy is attached to	policy	listEntitiesForDryRunPoli- cy
Querying effective policies	policy	showEffectivePolicies

Operation	Resource Type	Event Name
Adding a tag	accountorganizationUnitpolicyroottag	tagResource
Deleting a tag	accountorganizationUnitpolicyroottag	untagResource
Listing tags for the specified resource	accountorganizationUnitpolicyroottag	listTagsForResource
Listing roots, OUs, and accounts in an organization	entity	listEntities
Listing cloud services integrable with Organizations	service	listServices
Listing resource types that support tag policy enforcement	policy	listTagPolicyServices
Listing tags for the specified resource	accountorganizationUnitpolicyroottag	listTagResources
Adding tags to the specified resource	accountorganizationUnitpolicyroottag	createTagResource

Operation	Resource Type	Event Name
Deleting tags with a specified key from a specified resource	accountorganizationUnitpolicyroottag	deleteTagResource
Listing instances by resource type and tag	resourceInstance	listResourceInstances
Querying the number of instances by resource type and tag	resourceCount	showResourceInstances- Count
Querying project tags	tag	listResourceTags
Listing organization quotas	quota	listQuotas

9.2 Viewing CTS Traces in the Trace List

Scenarios

Cloud Trace Service (CTS) records operations performed on cloud service resources. A record contains information such as the user who performed the operation, IP address, operation content, and returned response message. These records facilitate security auditing, issue tracking, and resource locating. They also help you plan and use resources, and identify high-risk or non-compliant operations.

What Is a Trace?

A trace is an operation log for a cloud service resource, tracked and stored by CTS. Traces record operations such as adding, modifying, or deleting cloud service resources. You can view them to identify who performed operations and when for detailed tracking.

What Is a Management Tracker and Data Tracker?

A management tracker identifies and associates with all your cloud services, recording all user operations. It records management traces, which are operations performed by users on cloud service resources, such as their creation, modification, and deletion.

A data tracker records details of user operations on data in OBS buckets. It records data traces reported by OBS, detailing user operations on data in OBS buckets, including uploads and downloads.

Constraints

- Before the organization function is enabled, you can query the traces of a single account on the CTS console. After the organization function is enabled, you can only view multi-account traces on the Trace List page of each account, or in the OBS bucket or the CTS/system log stream configured for the management tracker with the organization function enabled. For details about organization trackers, see Organization Trackers.
- You can only query operation records of the last seven days on the CTS console. They are automatically deleted upon expiration and cannot be manually deleted. To store them for longer than seven days, configure transfer to Object Storage Service (OBS) or Log Tank Service (LTS) so that you can view them in the OBS buckets or LTS log streams.
- After creating, modifying, or deleting a cloud service resource, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.

Prerequisites

1. Register with Huawei Cloud and complete real-name authentication.

If you already have a Huawei Cloud account, skip this step. If you do not have one, do as follows:

- a. Log in to the Huawei Cloud official website, and click **Sign Up**.
- b. Sign up for a HUAWEI ID as prompted. For details, see Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services.
 - Your personal information page is displayed after the registration completes.
- Complete individual or enterprise real-name authentication by referring to Real-Name Authentication.

2. Grant permissions for users.

If you log in to the console using a Huawei Cloud account, skip this step. If you log in to the console as an IAM user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions. For details, see Assigning Permissions to an IAM User.

Viewing Traces

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, CTS starts recording user operations on data in OBS buckets. CTS retains operation records of the latest seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

Viewing Real-Time Traces in the Trace List of the New Edition

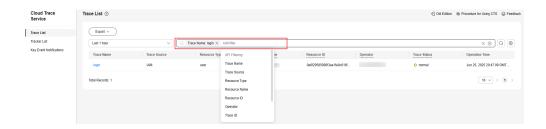
- **Step 1** Log in to the CTS console.
- **Step 2** In the navigation pane, choose **Trace List**.

- **Step 3** In the time range drop-down list above the trace list, select a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also select **Custom** to specify a custom time range within the last seven days.
- **Step 4** The search box above the trace list supports advanced queries. Combine one or more filters to refine your search.

Table 9-2 Trace filtering parameters

Parameter	Description
Read-Only	After selecting the Read-Only filter, you can select either Yes or No from the drop-down list.
	Yes: filters read-only operation traces, for example, resource query operations. This option is available after Read-Only Trace Reporting has been enabled in the Configuration Center and at least one read-only trace has been triggered.
	No: filters non-read-only operation traces, such as creating, modifying, and deleting resources.
Trace Name	Name of a trace.
	The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.
	For details about the operations that can be audited for each cloud service, see Supported Services and Operations.
	Example: updateAlarm
Trace Source	Cloud service name abbreviation.
	The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.
	Example: IAM
Resource	Name of a cloud resource involved in a trace.
Name	The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.
	If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty. Example: ecs-name
D ID	
Resource ID	ID of a cloud resource involved in a trace.
	The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported.
	Leave this field empty if the resource has no resource ID or if resource creation failed.
	Example: {VM ID}

Parameter	Description
Trace ID	Value of the trace_id parameter for a trace reported to CTS. The entered value requires an exact match. Fuzzy matching is not supported. Example: 01d18a1b-56ee-11f0-ac81-*****1e229
Resource Type	Type of a resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. For details about the resource types of each cloud service, see Supported Services and Operations. Example: user
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of trace_type in a trace is SystemAction, the operation is triggered by the service and the trace's operator may be empty. For details about the relationship between IAM identities and operators and the operator username format, see Relationship Between IAM Identities and Operators.
Trace Status	 Select one of the following options from the drop-down list: normal: The operation succeeded. warning: The operation failed. incident: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.
Enterprise Project ID	ID of the enterprise project to which a resource belongs. To check enterprise project IDs, go to the Enterprise Project Management Service (EPS) console and choose Project Management in the navigation pane. Example: b305ea24-c930-4922-b4b9-*****1eb2
Access Key	Temporary or permanent access key ID. To check access key IDs, hover over your username in the upper right corner of the console and select My Credentials from the pop-up list. On the displayed page, choose Access Keys in the navigation pane. Example: HSTAB47V9V ********TLN9



- **Step 5** On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.
 - Enter any keyword in the search box and press **Enter** to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
 - Click \bigcirc to view the latest information about traces.
 - Click to customize the information to be displayed in the trace list. If **Auto**wrapping is enabled (), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
- **Step 6** (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Traces in the Trace List of the Old Edition

- **Step 1** Log in to the CTS console.
- **Step 2** In the navigation pane, choose **Trace List**.
- **Step 3** Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.
- **Step 4** In the upper right corner of the page, set a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also click **Customize** to specify a custom time range within the last seven days.
- **Step 5** Set filters to search for your desired traces.

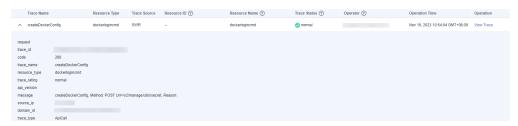
Table 9-3 Trace filtering parameters

Parameter	Description
Trace Type	Select Management or Data .
	 Management traces record operations performed by users on cloud service resources, including creation, modification, and deletion.
	Data traces are reported by OBS and record operations performed on data in OBS buckets, including uploads and downloads.
Trace Source	Select the name of the cloud service that triggers a trace from the drop-down list.
Resource type	Select the type of the resource involved in a trace from the drop-down list.
	For details about the resource types of each cloud service, see Supported Services and Operations.

Parameter	Description
Operator	User who triggers a trace.
	Select one or more operators from the drop-down list.
	If the value of trace_type in a trace is SystemAction , the operation is triggered by the service and the trace's operator may be empty.
	For details about the relationship between IAM identities and operators and the operator username format, see Relationship Between IAM Identities and Operators.
Trace Status	Select one of the following options:
	Normal: The operation succeeded.
	Warning: The operation failed.
	• Incident : The operation caused a fault that is more serious than a normal failure, for example, causing other faults.

Step 6 Click Query.

- **Step 7** On the **Trace List** page, you can also export and refresh the trace list.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
 - Click $\mathbb C$ to view the latest information about traces.
- **Step 8** In the **Tampered or Not** column of a trace, check whether the trace is tampered with.
 - **No**: The trace is not tampered with.
 - **Yes**: The trace is tampered with.
- **Step 9** Click $\stackrel{\vee}{}$ on the left of a trace to expand its details.



Step 10 Click **View Trace** in the **Operation** column. The trace details are displayed.

Step 11 (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

Helpful Links

- For details about the key fields in the trace structure, see Trace Structure and Example Traces.
- You can use the following examples to learn how to query a specific trace:
 - Use CTS to audit Elastic Volume Service (EVS) creation and deletion operations from the last two weeks. For details, see Security Auditing.
 - Use CTS to locate a fault or creation failure for an Elastic Cloud Server (ECS). For details, see Fault Locating.
 - Use CTS to check all operation records for an ECS. For details, see Resource Tracking.

10 Adjusting Quotas

What Is Quota?

A quota is a limit on the quantity or capacity of a certain type of service resources that a user can use, for example, the maximum number of OUs you can create or the number of member accounts you can invite to an organization.

If a quota cannot meet your needs, apply for a higher quota.

How Do I View My Quotas?

- 1. Log in to the Huawei Cloud console.
- Choose Resources > My Quotas in the upper right corner of the page.
 The Service Quota page is displayed.

Figure 10-1 My Quotas



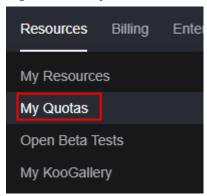
View the used and total quotas of each type of resources on the displayed page.

If a quota cannot meet your service requirements, apply for a higher quota.

How Do I Increase My Quota?

- 1. Log in to the management console.
- In the upper right corner of the page, choose Resources > My Quotas.
 The Service Quota page is displayed.

Figure 10-2 My Quotas



- 3. Click **Increase Quota**.
- On the Create Service Ticket page, set the parameters.
 In the Problem Description area, enter the required quota and the reason for the quota adjustment.
- 5. Read the agreements and confirm that you agree to them, and then click **Submit**.