ALIBABA CLOUD

Alibaba Cloud

Resource Management

Resource Directory

Document Version: 20220623

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Resource Directory overview

The Resource Directory service allows you to manage the relationships among a number of accounts and resources.

Scenarios

Resource Directory allows you to quickly establish an organizational structure based on your business requirements and consolidate the accounts of your enterprise into this structure to form a hierarchy for the resources of your enterprise. This way, you can manage your accounts and resources in a centralized manner. Resource Directory can meet your management requirements in aspects such as network deployment, settlement, user permissions, security compliance, and log auditing. The following descriptions provide the use scenarios of Resource Directory:

- **Business environment-based creation of organizational structures**

  Your enterprise may have various branches, departments, or projects. Resource Directory allows you to build an organizational structure on the cloud based on your business environment.

- **Centralized management of all Alibaba Cloud accounts and resources**

  If your enterprise has multiple Alibaba Cloud accounts, you can enable a resource directory and place the accounts in it. This way, you can manage the accounts and the resources within them in a centralized manner.

- **Centralized management of bills and invoices**

  You can create a member in your resource directory and use this member for the settlement of all bills and invoices. After an account joins your resource directory, you can change the billing account of the account to facilitate bill management.

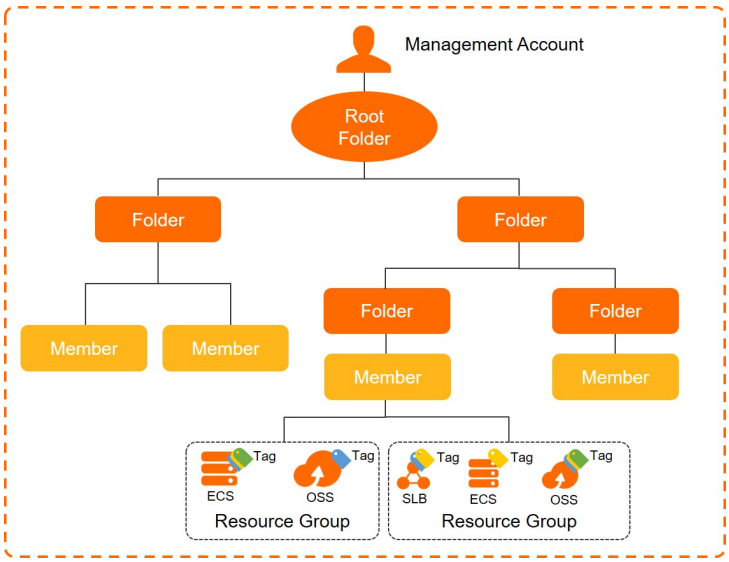
- **Implementation of permission and compliance requirements**

  You can configure different resource access rules for different accounts and directory structures by using the policies of Resource Access Management (RAM) and the access control policies of Resource Directory. This enables the authorization and management channel between personnel and resources and ensures the security of the resources.

- **Integration with a variety of enterprise-level Alibaba Cloud applications**

  Resource Directory is integrated with the Alibaba Cloud finance, compliance auditing, cloud security, and network platforms. This way, you can use the same organizational structure to manage all your enterprise accounts and resources.

Terms



Term	Description
management account	A management account is an account that is used to enable a resource directory and is the super administrator of the resource directory. The management account has all administrative permissions on the resource directory and the members in the resource directory. Only an Alibaba Cloud account that has passed enterprise real-name verification can be used as a management account. Each resource directory has only one management account. To ensure the security of the management account, we recommend that you create an Alibaba Cloud account and use this Alibaba Cloud account as the root user of the management account. Do not use an existing Alibaba Cloud account to enable a resource directory. In addition, you can create a RAM user for the management account, grant administrator permissions to the RAM user, and use this RAM user to manage the entire resource directory. Only the management account of a resource directory or a RAM user that has administrator permissions can be used to perform operations in the resource directory. **Note** A management account does not belong to a resource directory and is not limited by the access control policies of a resource directory.
Root folder	The Root folder is the parent folder of all the other folders in a resource directory. These folders are organized in a hierarchy that starts from the Root folder.
folder	A folder is an organizational unit in a resource directory. A folder may indicate a branch, line of business, or project of an enterprise. Each folder can contain members and subfolders, which forms a tree-shaped organizational structure.

Term	Description
member	A member serves as a container for resources and is also an organizational unit in a resource directory. A member indicates a project or application. The resources of different members are isolated. You can use a management account to grant the required permissions to a RAM user or RAM role and use this RAM user or RAM role to log on to or access members. The following types of members are supported: • Resource account A member that you create in a resource directory is a resource account. Root permissions are not granted to resource accounts. Therefore, resource accounts provide higher security. For more information about how to create a resource account, see Create a member. • Cloud account A cloud account is another name for an Alibaba Cloud account in a resource directory. You can invite an existing Alibaba Cloud account to join your resource directory. Cloud accounts have root permissions. For more information about how to invite an Alibaba Cloud account to join a resource directory, see Invite an Alibaba Cloud account to join a resource directory.
RDP	A resource directory path (RDP) indicates the location of a resource entity (folder or member) in a resource directory. The RDP of a resource entity consists of the ID of the resource entity, the IDs of all the parent folders of the resource entity, and the ID of the resource directory to which the resource entity belongs. An RDP is in one of the following formats: • RDP of a folder: `<ID of the resource directory to which the folder belongs>/<ID of the Root folder in the resource directory>/.../<ID of the folder>`. • RDP of a member: `<ID of the resource directory to which the member belongs>/<ID of the Root folder in the resource directory>/.../<ID of the member>`. For example, the RDP of the member 181761095690**** is `rd-r4****/r-oG****/fd-RIErN0****/fd-XVxh6D****/181761095690****`. For more information about how to view the RDP of a folder or member, see View the basic information of a folder or View the detailed information of a member.

Procedure

1. Log on to the Resource Management console by using an account that can be used as a management account.
2. Enable a resource directory.

   For more information, see Enable a resource directory.
3. Create folders to build an organizational structure for your enterprise.

For more information, see Create a folder.

4. Create members in the resource directory or invite existing Alibaba Cloud accounts to join the resource directory. Then, move all members to the folders that you created based on your business requirements.

   For more information, see Create a member, Invite an Alibaba Cloud account to join a resource directory, and Move a member.

Limits

Item	Upper limit	Adjustable	Remarks
Number of resource directories that you can create by using an Alibaba Cloud account	1	N/A	The members of a resource directory cannot be used to create resource directories.
Number of Root folders in a resource directory	1	N/A	None.
Number of folders in a resource directory	100	Apply for a quota.	The Root folder is not included.
Number of folder levels	5	N/A	The Root folder is not included.
Number of members in a resource directory	20	Apply for a quota.	None.
Number of valid invitations per day	20	Apply for a quota.	Accepted invitations are not included.
Duration of invitation expiration	14 days	N/A	None.
Number of verification codes that can be sent per day when you bind a mobile phone number to a member for security purposes	100	N/A	None.

2.Manage a resource directory

2.1. Enable a resource directory

The Resource Management service allows you to consolidate all your Alibaba Cloud accounts into a resource directory and move the accounts to related folders to form a hierarchy. This way, you can manage the accounts and the resources within the accounts in a unified manner. You must enable a resource directory before you can use the resource directory.

Prerequisites

The Alibaba Cloud account you use to enable a resource directory has passed enterprise real-name verification. An account that has passed only individual real-name verification cannot be used to enable a resource directory.

Methods used to enable a resource directory

By default, an Alibaba Cloud account that is used to enable a resource directory is the management account of the resource directory. The management account has all administrative permissions on the resource directory and can be used to manage all members in the resource directory and the resources of the members. We recommend that you use an Alibaba Cloud account only as the management account of a resource directory and do not use the account to deploy your business. This prevents management issues caused by the excessive responsibilities of the management account.

When you use an Alibaba Cloud account to enable a resource directory, the system checks whether the account has passed enterprise real-name verification, whether the account has resources, and whether the account is configured with security information, such as a mobile phone number or an email address. If the account meets requirements, the system then recommends one of the following methods for you to enable a resource directory based on the check results:

- Use the current account to enable a resource directory

  You can use this method to enable a resource directory if your account has passed enterprise real-name verification, is configured with security information, and does not have resources.

- Use a new account to enable a resource directory

  You can use this method to enable a resource directory if your account has passed enterprise real-name verification but is not configured with security information or has resources. If you use this method, you must create an Alibaba Cloud account and use this account as the management account of the resource directory. The new account inherits the enterprise real-name verification information of the current account. The current account becomes a member of the resource directory.

Use the current account to enable a resource directory

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. On the page that appears, click **Enable Resource Directory**.
4. On the Confirm Management Account page, select **Current Account**.
5. Click **Enable**.
6. In the **Security Verification** dialog box, enter the verification code that is sent to the mobile phone number or email address bound to the current account and click **OK**.

After you enable the resource directory, the system creates a **Root** folder and uses the current account as the management account of the resource directory.

In addition, the system creates a service-linked role named AliyunServiceRoleForResourceDirectory within the management account. This role is used to grant access permissions on the resource directory to trusted services that are integrated with the Resource Directory service. For more information about service-linked roles, see Service-linked role for Resource Directory.

Use a new account to enable a resource directory

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. On the page that appears, click **Enable Resource Directory**.
4. On the Confirm Management Account page, select **New Account**.
5. Enter a custom account name in the Account Name field.
6. Bind a mobile phone number to the new account for security purposes.

   The mobile phone number that is bound to the current account is automatically displayed. You can click **Modify** to bind another mobile phone number to the new account for security purposes.
7. Click **Enable**.
8. In the **Security Verification** dialog box, enter the verification code that is sent to the mobile phone number you specify in Step and click **OK**.

   After you enable the resource directory, the system creates a **Root** folder and uses the new account as the management account of the resource directory. The current account becomes a member of the resource directory.

   > **Note** You must set a password for the management account on the password resetting page by using the mobile phone number that you specify in Step . Then, you can use the management account to log on to the Resource Management console to manage your resource directory.

   In addition, the system creates a service-linked role named AliyunServiceRoleForResourceDirectory within the management account. This role is used to grant access permissions on the resource directory to trusted services that are integrated with the Resource Directory service. For more information about service-linked roles, see Service-linked role for Resource Directory.

2.2. View the basic information of a resource directory

This topic describes how to view the basic information of a resource directory. The information includes the ID, creation time, and management account of the resource directory.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Configure**.
3. View the basic information of the resource directory. The information includes the ID, creation time, and management account of the resource directory.

2.3. Disable a resource directory

If you no longer need a resource directory, you can disable it. This operation cannot be undone. Therefore, proceed with caution.

Prerequisites

The resource directory that you want to disable does not contain the following items:

- Members
- Folders except the **Root** folder

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Configure**.
3. In the Disable Resource Directory section, click **Disable Resource Directory**.

Result

After a resource directory is disabled, the following events occur:

- The organizational structure and policies created in this resource directory are cleared.
- Data in trusted services that are activated are cleared. For example, if you create a multi-account trail in ActionTrail, the data of the multi-account trail in ActionTrail will be cleared after you disable your resource directory.
- Services that depend on the organizational structure may be unavailable.
- The management account becomes an independent Alibaba Cloud account. You can use this account to create another resource directory.

2.4. Service-linked role for Resource Directory

This topic describes the use scenarios, permission policies, creation, and deletion of the service-linked role for the Resource Directory service. This role is named AliyunServiceRoleForResourceDirectory.

Scenarios

The AliyunServiceRoleForResourceDirectory role provides a trusted access channel for services that are integrated with Resource Directory. Resource Directory can assume this role and create service-linked roles for these integrated services. This way, Resource Directory can access cloud services that are associated with the integrated services.

For more information, see Service-linked roles.

Role description

Role name: AliyunServiceRoleForResourceDirectory.

Permission policy: AliyunServiceRolePolicyForResourceDirectory.

Permissions: This role can be used to create or delete service-linked roles for services that are integrated with Resource Directory.

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": "ram:CreateServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "resourcemanager.aliyuncs.com"
                }
            }
        }
    ]
}
```

Create the service-linked role for Resource Directory

The system automatically creates the AliyunServiceRoleForResourceDirectory role in the following scenarios:

- Creates the role within the management account of a resource directory after the resource directory is enabled.
- Creates the role within a member of a resource directory after the member is created in the resource directory.
- Creates the role within an invited account after the invited account joins a resource directory.

Delete the service-linked role for Resource Directory

The system attempts to automatically delete the AliyunServiceRoleForResourceDirectory role in the following scenarios:

- Deletes the role within the management account of a resource directory when the resource directory is disabled.
- Deletes the role within a member of a resource directory when the member is deleted from the resource directory.

If the role is not used by cloud resources, you can manually delete the role. For more information, see Delete a RAM role.

3.Manage folders

3.1. Create a folder

A folder is an organizational unit in a resource directory. You can use folders to build an organizational structure for resources.

Context

You can create subfolders in a folder. A maximum of five levels of folders can be created in the Root folder.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** tab.
4. In the left-side navigation tree, click the name of a folder. In the right-side section that appears, click **Create Folder**.

   A subfolder will be created in the folder.
5. In the **Create Folder** panel, specify **Folder Name**.

   > **Note** The name must be unique in the current resource directory.
6. Click **OK**.

What's next

You can create member accounts in a folder and manage them in a unified manner. For more information, see Create a member.

3.2. View the basic information of a folder

This topic describes how to view the basic information of a folder, including the name, ID, creation time, resource directory (RD) path, and members of the folder.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** tab.
4. In the left-side navigation tree, find the folder whose basic information you want to view and click the folder name. In the section that appears, you can view the basic information of the folder, including the name, ID, creation time, RD path, and members of the folder.

   > **Note** For more information about an RD path, see Terms.

3.3. Change the name of a folder

This topic describes how to change the name of a folder.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** tab.
4. In the left-side navigation tree, find the folder whose name you want to change and click the folder name.
5. In the right-side section that appears, move the pointer over the folder name and click the icon.
6. In the dialog box that appears, change the name and click **OK**.

> **Note** The name must be unique in the current resource directory.

3.4. Delete a folder

If a folder does not contain member accounts or subfolders, you can delete it. A deleted folder cannot be recovered. Therefore, exercise caution when you delete a folder.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** tab.
4. In the left-side navigation tree, find the folder that you want to delete and click the folder name.
5. In the right-side section that appears, click **Delete Folder**.

> **Note** The **Delete Folder** button is displayed only when no member accounts or subfolders exist in a folder.

6. In the **Delete Folder** message, click **OK**.

4.Manage member accounts

4.1. Create a member

Members are resource containers in a resource directory and serve as organizational units in the resource directory. The members isolate resources. You can create members in folders and manage the members in a centralized manner.

Context

- For more information about the limit on the number of members that can be created in a resource directory, see Limits on resource directories.
- You can use one of the following methods to create a member:
  - In the left-side navigation pane of the Resource Management console, choose **Resource Directory > Overview**. On the **Organization** tab of the page that appears, create a member in an existing folder. Alternatively, you can create a folder and create a member in the new folder. This topic describes this method.
  - In the left-side navigation pane of the Resource Management console, choose **Resource Directory > Overview**. On the page that appears, click the **Members** tab. On this tab, click Create Member to create a member. The created member belongs to the Root folder by default. You can move the member to your desired folder. For more information about how to move a member, see Move a member.
  - In the left-side navigation pane of the Resource Management console, choose **Resource Directory > Create Member**. On the page that appears, create a member. The created member belongs to the Root folder by default. You can move the member to your desired folder. For more information about how to move a member, see Move a member.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. On the **Organization** tab, find the folder in which you want to create a member and click the folder name.
4. In the right-side section that appears, click **Create Member**.
5. On the **Create Member** page, configure the **Alibaba Cloud Account Name** parameter.

   The Alibaba Cloud account name that is specified for a member must be unique in the current resource directory. The name must be 2 to 50 characters in length and can contain letters, digits, underscores (_), periods (.), and hyphens (-). The name must start and end with a letter or digit. The name cannot contain consecutive special characters.
6. Configure the **Display Name** parameter.

   The display name of a member must be 2 to 50 characters in length and can contain letters, digits, underscores (_), periods (.), and hyphens (-).
7. Configure the **Settlement** parameter.
   - **Use the Management Account to pay for new member**: If you select this option, the management account of the resource directory is used as the billing account of the member that is being created.

- **Use existing member to pay for new member**: If you select this option, you must select an existing member from the panel that appears. This member is used as the billing account of the member that is being created.

  > **Note**
  >
  > A member that does not have the payment capability cannot be selected. For more information about how to determine whether a member has the payment capability, see Consolidated Billing Overview.

- **New member pay by themselves**: If you select this option, the member that is being created is used as its billing account.

8. Click **OK**.

> **Note** Members created in a resource directory inherit the legal entity of the management account for the resource directory. This indicates that the real-name verification information of the members is consistent with the real-name verification information of the management account.

Result

After members are created in a resource directory, the system manages them in a centralized manner.

- The system automatically activates the Resource Access Management (RAM) service for the members.
- The system automatically creates a RAM role named ResourceDirectoryAccountAccessRole for each member and assigns the role to the management account of the resource directory. This way, you can use the management account to manage the members in a centralized manner.
- Each member belongs to only one folder. You can use the management account to move members between folders in the resource directory based on your business requirements. After a member is moved from one folder to another, the resources within the member are also moved to the new folder.

4.2. Invite member accounts

4.2.1. Invite an Alibaba Cloud account to join a resource directory

You can invite Alibaba Cloud accounts to join your resource directory to manage them in a centralized manner.

Prerequisites

Before you initiate an invitation, make sure that the following requirements are met:

- The Alibaba Cloud account that you want to invite does not have a pending invitation. An Alibaba Cloud account that has a pending invitation cannot be invited again.
- Less than 20 invitations are initiated on the current day. A maximum of 20 invitations can be initiated per day.
- Less than 20 invitations are in the **Pending Confirmation** state. Otherwise, you cannot initiate an

invitation.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Invite Member**.
3. On the Invite Member page, click **Invite Member**.
4. In the Invite Member panel, configure the Account ID/Logon Email parameter.

   > **Note** If you want to enter the email address of an Alibaba Cloud account, you must enter the email address that you specified when you created the account. You can enter multiple account IDs or email addresses. Separate the account IDs or email addresses with commas (,).

5. Configure the **Remarks** parameter.

   > **Note** The remarks help the invitee confirm the credibility of the invitation and quickly complete the invitation process.

6. Read the risk warning and select the check box.
7. Click **OK**.

   > **Note**
   > - If you enter an email address for an invitation, the system sends a confirmation email to the email address.
   > - If you enter an account ID for an invitation, the system sends a confirmation email to the email address that is associated with the account.
   > - If you enter an account ID for an invitation but no email address is associated with the account, the invitee can log on to the Resource Management console to view and process the invitation.

Result

After the invited Alibaba Cloud account joins your resource directory, it becomes a member of the resource directory and is managed by the resource directory.

- By default, the name of the Alibaba Cloud account is used as the display name of the member in the resource directory. You can use the management account of the resource directory to change the display name of the member but cannot change the name of the Alibaba Cloud account.
- The system creates a RAM role named ResourceDirectoryAccountAccessRole for the member and assigns the role to the management account of the resource directory for centralized management.
- You can use the management account of the resource directory to change the location of the member in the resource directory.

4.2.2. View information of an invitation

After you initiate an invitation, you can view information of the invitation in the Resource Management console. The information includes the ID, creation time, and status of the invitation as well as the account ID or email address of the invitee.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Invite Member**.
3. View the information of an invitation.
   - **Invitation ID**: the ID of an invitation. The ID is automatically generated by the system.
   - **Account ID/Logon Email**: the Alibaba Cloud account ID or email address of an invitee.
   - **Invitation Time**: the time when an invitation was initiated.
   - **Expiration Time**: the time when an invitation will become invalid. An invitation is valid for 14 days.
   - **Status**: the state of an invitation. An invitation has the following states: **Pending**, **Canceled**, **Accepted**, **Declined**, and **Expired**.
   - **Description**: the remarks that were entered when an invitation was initiated.
   - **Actions**: You can click **Cancel Invitation** to cancel an invitation in the **Pending** state.

     > **Note** The system automatically deletes invitations 30 days after these invitations become invalid.

4.2.3. Process an invitation

After you receive an invitation, you can view the information about the invitation in the Resource Management console or in your email. Then, you can accept or reject the invitation.

Prerequisites

- The invited Alibaba Cloud account is not the management account or a member of a resource directory. One Alibaba Cloud account can belong to only one resource directory.
- The invited Alibaba Cloud account has passed enterprise real-name verification. An Alibaba Cloud account that has not passed enterprise real-name verification or passes individual real-name verification cannot join a resource directory.
- If you want to use a RAM user to process the invitation, the policy with the minimum required permissions is attached to the RAM user. The following code provides the policy document:

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resourcemanager:GetResourceDirectory",
                "resourcemanager:ListHandshakesForAccount",
                "resourcemanager:GetHandshake",
                "resourcemanager:AcceptHandshake",
                "resourcemanager:DeclineHandshake"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see Create a custom policy and Grant permissions to a RAM user.

Context

Before you accept the invitation, carefully read the following information and make sure that you are familiar with the risks that may arise. After you accept the invitation, the following situations occur:

- Your Alibaba Cloud account becomes a member of the cloud account type in the resource directory, and the name of your Alibaba Cloud account is used as the display name of the member in the resource directory.
- The management account of the resource directory has all permissions on your Alibaba Cloud account, and you cannot remove your Alibaba Cloud account from the resource directory.
- For security or compliance purposes, the management account of the resource directory can be used to attach one or more access control policies to your Alibaba Cloud account to determine the cloud services and API operations that you can access by using the Alibaba Cloud account.
- The management account of the resource directory or a delegated administrator account of a trusted service can be used to perform specific administrative operations on your Alibaba Cloud account in the trusted service. For example, the management account or a delegated administrator account of the trusted service ActionTrail can be used to view the log data of your Alibaba Cloud account in ActionTrail, and the management account or a delegated administrator account of the trusted service Resource Orchestration Service (ROS) can be used to quickly deploy cloud resources for your Alibaba Cloud account in ROS. For more information, see Overview.
- If the enterprise real-name information of your Alibaba Cloud account is the same as that of the management account of the resource directory, the management account can be used to switch the member from a cloud account to a resource account. Otherwise, the member cannot be switched from a cloud account to a resource account.

Accept an invitation

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. On the page that appears, click **View Invitation**.
4. On the page that appears, find the invitation that you want to accept and click **Process Invitation** in the **Actions** column.

5. In the **Process Invitation** dialog box, carefully read the invitation information, select the risk warning check box, and then click **Accept Invitation**.
   After your account joins the resource directory, you can view the information about the resource directory on the **Settings** page.

Reject an invitation

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. On the page that appears, click **View Invitation**.
4. On the page that appears, find the invitation that you want to reject and click **Process Invitation** in the **Actions** column.
5. In the **Process Invitation** dialog box, click **Reject Invitation**.
6. In the **Reject Invitation** dialog box, click **Reject Invitation**.

4.3. View the detailed information of a member

This topic describes how to view the detailed information of a member. The information includes the member type, member name, Alibaba Cloud account name, Alibaba Cloud account ID, real-name verification information, settlement account, status, and resource directory (RD) path.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** or **Members** tab.
4. Find the member whose detailed information you want to view and click the name of the member.
5. In the **Member Details** panel, view the following information: member type, member name, Alibaba Cloud account name, Alibaba Cloud account ID, real-name verification information, settlement account, status, and RD path.

   > **Note** For more information about an RD path, see Terms.

4.4. Change the display name of a member

This topic describes how to change the display name of a member. The display name of a member must be unique in a resource directory.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** or **Members** tab. Then, find the member whose display name you want to

change and click the display name of the member.

4. In the Member Details panel, move the pointer over the display name of the member and click the edit icon.
5. Enter a new display name for the member in the field that appears and click **OK**.

4.5. Move a member

You can move a member between folders in a resource directory and adjust the resources within the member to meet your business requirements.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** or **Members** tab.
4. Find the member that you want to move and click **Move** in the **Actions** column.
5. In the **Move Member** panel, select the destination folder and click **OK**.

Result

You can then view the member in the destination folder.

4.6. Access a member

You can use a RAM role, a RAM user, or the root user to access members. For security purposes, we recommend that you use a RAM role or RAM user to access members.

Use a RAM role to access a member

The system automatically creates a RAM role named ResourceDirectoryAccountAccessRole for each member in a resource directory. The trusted entity of the role is the management account of the resource directory. You can use the management account or a RAM user of the management account to assume the ResourceDirectoryAccountAccessRole role of a member and access the member.

1. Create a RAM user by using the management account.

   In this example, the RAM user Alice is created. For more information, see Create a RAM user.

2. Grant permissions to Alice.

   You must grant the following permissions to Alice:

   - AliyunSTSAssumeRoleAccess: the permission to call the AssumeRole operation of Security Token Service (STS)
   - AliyunResourceDirectoryFullAccess: the permission to manage a resource directory

   > **Note** If you want to use Alice as an administrator, you can grant the AdministratorAccess permission to Alice.

   For more information about how to grant permissions to a RAM user, see Grant permissions to a RAM user.

3. Use Alice to log on to the Resource Management console.

4. In the left-side navigation pane, choose **Resource Directory > Overview**.
5. Click the **Organization** or **Members** tab.
6. Find the member that you want to access and click **Logon Account** in the **Actions** column.

   Then, you can use Alice to assume the RAM role ResourceDirectoryAccountAccessRole of the member and perform the operations that are defined for the RAM role.

Use a RAM user to access a member

You can create a RAM user for a member and use this RAM user to log on to the Alibaba Cloud Management Console and access the member.

1. Use a RAM user that belongs to the management account to assume the related RAM role and access a member.

   For more information, see Use a RAM role to access a member.
2. Create a RAM user for the member.

   In this example, the RAM user Tom is created. For more information, see Create a RAM user.
3. Grant permissions to Tom.

   If you want to access all the resources of a member, grant the AdministratorAccess permission to Tom. In other cases, grant permissions to Tom based on your business requirements. For more information, see Grant permissions to a RAM user.
4. Use Tom to log on to the Alibaba Cloud Management Console.

   For more information, see Log on to the Alibaba Cloud Management Console as a RAM user.

Use the root user to access a member

You can use the root user to log on to the Alibaba Cloud Management Console and access the member.

> **Note** For security purposes, we recommend that you do not use the root user to access members.

1. Log on to the Alibaba Cloud Management Console.

   > **Note** If you have logged on to the Alibaba Cloud Management Console by using another account, log off from the console first.
2. Enter the username and password of your account.
3. Click **Sign In**.

4.7. Bind a mobile phone number to a resource account

A mobile phone number is used to verify the identity of a user on the cloud and receive important change notifications. For example, a mobile phone number can be used to receive notifications about password resetting, instance or cluster release, and fee changes. This topic describes how to bind a mobile phone number to a resource account.

Prerequisites

A RAM user or RAM role is created within the management account of your resource directory, and the AliyunResourceDirectoryFullAccess policy is attached to the RAM user or RAM role. You must use such a RAM user or RAM role to perform operations described in this topic. This ensures that the system can record the operators of management operations.

Limits

- You cannot bind a mobile phone number to a cloud account in the Resource Management console. If you want to bind a mobile phone number to a cloud account, go to the Security Settings page.
- You can refer to this topic only to bind a mobile phone number to a resource account. You cannot refer to this topic to modify the mobile phone number that is bound to a resource account.
- A maximum of 100 verification codes can be sent per day.

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** or **Members** tab.
4. Find the resource account to which you want to bind a mobile phone number and click **Bind secure mobile phone** in the **Actions** column.
5. In the **Bind secure mobile phone number** dialog box, enter a mobile phone number in the Mobile phone number field, click Get verification code to obtain a verification code, and then enter the code in the Verification code field.
6. Click **OK**.

4.8. Switch a resource account to a cloud account

If you must use the root user of a resource account to perform operations, you can switch the resource account to a cloud account. After you perform the operations, we recommend that you switch the cloud account back to a resource account at the earliest opportunity to ensure security.

Prerequisites

- A RAM user or RAM role is created within the management account of your resource directory, and the AliyunResourceDirectoryFullAccess policy is attached to the RAM user or RAM role. You must use such a RAM user or RAM role to perform operations described in this topic. This ensures that the system can record the operators of management operations.
- A mobile phone number is bound to the resource account for security purposes. If no mobile phone number is bound to the resource account, you cannot switch it to a cloud account. For more information, see Bind a mobile phone number to a resource account.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** or **Members** tab.
4. Find the resource account that you want to switch and click **Switch to Cloud Account** in the **Actions** column.
5. In the **Switch to Cloud Account** dialog box, read the risk warning, select the risk warning check

box, and then click **OK**.

Result

After the resource account is switched to a cloud account, you can use the root user of the cloud account to log on to the Alibaba Cloud Management Console.

You can use the password retrieval feature to reset the password of the root user and use the root user to log on to the Alibaba Cloud Management Console. If you have specified a password for the root user, you can directly use the password.

After the root user is enabled, the security risks of the cloud account increase. Keep the account and password of the root user secure.

4.9. Switch a cloud account to a resource account

After you invite an Alibaba Cloud account to join your resource directory and the owner of the Alibaba Cloud account accepts the invitation, the Alibaba Cloud account becomes a member of the cloud account type in the resource directory. By default, the root user of an Alibaba Cloud account is enabled and has full permissions. If the account and password of the root user are leaked, irreparable losses will occur. For security purposes, we recommend that you switch the cloud account to a resource account.

Prerequisites

- A RAM user or RAM role is created within the management account of your resource directory, and the AliyunResourceDirectoryFullAccess policy is attached to the RAM user or RAM role. You must use such a RAM user or RAM role to perform operations described in this topic. This ensures that the system can record the operators of management operations.
- The cloud account that you want to switch to a resource account must meet the following requirements:
  - The real-name information of the cloud account is the same as that of the management account of the resource directory.
  - Security information, such as a mobile phone number or an email address, is specified for the cloud account.
  - The cloud account does not have AccessKey pairs in use.

    If the cloud account has an AccessKey pair in use, go to the AccessKey Management page to disable the AccessKey pair.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** or **Members** tab.
4. Find the cloud account that you want to switch and click **Switch to Resource Account** in the **Actions** column.
5. In the **Switch to Resource Account** dialog box, read the risk warning, select the risk warning check box, and then click **OK**.
6. In the **Security Verification** dialog box, click Get verification code to obtain a verification code,

enter the verification code in the Verification code field, and then click **OK**.

Result

After the cloud account is switched to a resource account, you cannot use the root user of the resource account to log on to the Alibaba Cloud Management Console. You can use the management account of the resource directory to create a RAM user and grant the RAM user the minimum required permissions to access the member.

4.10. Remove a member

You can remove members of the cloud account type from your resource directory.

Prerequisites

If a member is a delegated administrator account of a trusted service, the member cannot be directly removed from your resource directory. You must remove the delegated administrator account for the trusted service first. For more information, see Remove a delegated administrator account.

Context

In a resource directory, members of the resource account type are resource containers that are created by using the management account of the resource directory. You cannot remove such members from the resource directory. For security purposes, you can use these members only within the resource directory.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Overview**.
3. Click the **Organization** or **Members** tab.
4. Find the member that you want to remove and click **Remove** in the **Actions** column.
5. In the **Remove Member** message, click **OK**.
   After you remove the member from the resource directory, the following changes occur:
   - The member becomes an independent Alibaba Cloud account. The account is no longer managed by the management account of the resource directory and limited by the access control policies of the resource directory.
   - The payment relationship of the account remains unchanged. If you want to update the payment relationship of the account, go to the financial system.

5.Manage control policies

5.1. Overview

The Control Policy feature provided by the Resource Directory service allows you to manage the permission boundaries of the folders or members in a resource directory in a centralized manner. This feature is implemented based on the resource directory. You can use this feature to develop common or dedicated rules for access control. The Control Policy feature does not grant permissions but only defines permission boundaries. Before you use an account that is a member of your resource directory to access resources, you must grant the required permissions to the account by using the Resource Access Management (RAM) service.

Scenarios

After an enterprise creates a resource directory and creates members in the resource directory for all departments, the enterprise must manage the use of these members. Otherwise, O&M rules may be violated, which results in security risks and superfluous costs. The resource directory provides the Control Policy feature. This feature enables the enterprise to formulate access control policies in a centralized manner by using the management account of the resource directory. The enterprise can then attach these policies to the folders and members in the resource directory. These policies control access to the resources that belong to the members. This ensures security compliance and controllable costs. For example, the enterprise is not allowed to use a member to apply for domain names or delete log records.

Types of access control policies

- **System access control policy**

  Resource Directory provides only one system access control policy, which is FullAliyunAccess. You can view the system access control policy but cannot create, modify, or delete it. After you enable the Control Policy feature, the system attaches the system access control policy to all the folders and members in your resource directory by default. This policy allows all operations on all your cloud resources.

- **Custom access control policy**

  Custom access control policies are customized by users. You can create, modify, or delete custom access control policies. After you create a custom access control policy, you must attach the policy to folders or members for the policy to take effect. If you no longer require the custom access control policy, you can detach it from the folders or members.

How it works

The Control Policy feature works in the following way:

1. Use the management account of your resource directory to enable the Control Policy feature. For more information, see Enable the Control Policy feature.

   After the feature is enabled, the system attaches the system access control policy FullAliyunAccess to all the folders and members in your resource directory by default. This policy allows all operations on all your cloud resources. This prevents resource access failures caused by inappropriate control policy configurations.

2. Use the management account of your resource directory to create a custom access control policy.

For more information, see Create a custom access control policy.

3. Use the management account of your resource directory to attach the newly created custom access control policy to folders or members in the resource directory. For more information, see Attach a custom access control policy.

   Access control policies can be attached to all folders or members in your resource directory. If you attach a custom access control policy to a folder, this policy also applies to all subfolders of the folder. For example, you attach Policy A to a folder and Policy B to one of its subfolders. In this case, both policies apply to the subfolder and all the members in the subfolder.

   > **Note** We recommend that you first attach a custom access control policy to only a few folders or members to check whether the policy can take effect as expected. If the custom access control policy takes effect as expected, you can attach it to all the other folders or members in your resource directory.

4. When a RAM user or RAM role of a member accesses an Alibaba Cloud service, the system matches the access request with the custom access control policy and verifies the permissions of the RAM user or RAM role.
   - The system matches the access request with custom access control policies level by level in reverse order based on the resource directory. The matching starts from the member that manages the resource the RAM user or RAM role wants to access.
   - If a Deny access control policy is matched, the system terminates access control policy matching, does not verify the permissions of the RAM user or RAM role, and then denies the access request.
   - If no Deny or Allow access control policy is matched, the system terminates access control policy matching, does not verify the permissions of the RAM user or RAM role, and then denies the access request.
   - If no Deny access control policy is matched but an Allow access control policy is matched, the system matches the access request with the access control policies that are attached to an upper-level object. The matching ends when the Root folder is matched. If the Root folder passes the matching, the whole resource directory passes the matching. Then, the system verifies the permissions of the RAM user or RAM role. For more information, see Policy evaluation process.
   - Access control policies do not apply to service-linked roles. For more information about service-linked roles, see Service-linked roles.
   - When you access a member, the system evaluates both the access control policies that are attached to the member and the access control policies that are attached to all its parent folders. This ensures that the access control policies that are attached to a folder take effect on all the members in the folder and all the members in the subfolders of the folder.

   > **Note** The access control policies that are configured within a resource directory also take effect for all the RAM users and RAM roles of the resource accounts and cloud accounts in the resource directory. However, the policies do not take effect for the root users of cloud accounts.

Configure an existing custom access control policy to allow access from specific Alibaba Cloud services

Custom access control policies limit the permissions on access to the resources of the members to which the access control policies are attached. The permissions that are specified in the access control policies are prohibited. As a result, some Alibaba Cloud services may fail to access the resources.

Alibaba Cloud services may use service roles to access the resources of your account to implement some features. If the permissions of the service roles are prohibited by access control policies, some features of the services cannot be used. If this is exactly what you expect from the access control policies, no operations are required. Otherwise, perform the following steps:

1. Determine the name of the service role used by the service for which you do not want to control access.

   You can log on to the RAM console to view all the service roles of your account.

2. Add the `"acs:PrincipalArn"` key to the `Condition` parameter in the document of the policy that controls the access from the service. Then, specify the determined role name for the key. The following code provides an example:

```
{
    "Statement": [
        {
            "Action": [
                "ram:UpdateUser"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN":"acs:ram:*:*:role/<Name of the service role>"
                }
            }
        }
    ],
    "Version": "1"
}
```

   For more information about the syntax of access control policies, see Languages of access control policies.

Limits

Item	Upper limit
Number of custom access control policies that can be created in a resource directory	1,500
Number of custom access control policies that can be attached to each folder or member	10
Number of characters that each custom access control policy can contain	4,096

Alibaba Cloud services that do not support the Control Policy feature

This section provides the Alibaba Cloud services that do not support the Control Policy feature. You must pay attention to control risks. If you want to control access to the services, contact the service manager of Resource Directory.

- Microservices Engine (MSE) does not support the Control Policy feature.
- The following applications and clusters in Message Queue for Apache RocketMQ do not support the Control Policy feature:
  - The mq-http application does not support the Control Policy feature and will be deprecated.
  - The onsbroker application does not support the Control Policy feature in the following regions:
    - UAE (Dubai).
    - China (Shanghai): The sh-share9 and shvip-st21ujm8f01 clusters in this region do not support the Control Policy feature.
    - China North 2 Ali Gov 1: The beijing.gov.vip.v0h0ovmfp02, beijing.gov.vip.nif1zmrlf02, and vip-cn-north-2-gov-1-45914plw301 clusters in this region do not support the Control Policy feature. The beijing.gov.vip.v0h0ovmfp02 and beijing.gov.vip.nif1zmrlf02 clusters will be deprecated.

5.2. Enable the Control Policy feature

The Control Policy feature is disabled by default. You can use this feature after you enable it.

Context

After the Control Policy feature is enabled, a resource directory has the following changes:

- The system automatically attaches the system access control policy FullAliyunAccess to folders and members in the resource directory. This policy allows all operations on all your cloud resources.
- When you create a folder or member, the system automatically attaches the system access control policy FullAliyunAccess to the folder or member.
- After an invited Alibaba Cloud account joins a resource directory, the system automatically attaches the system access control policy FullAliyunAccess to this member.
- When you remove a member, the system automatically detaches all access control policies that are attached to this member.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. In the upper part of the Control Policy page, click **Enable Control Policy**.
4. In the message that appears, click **OK**.
5. Click the **Refresh** icon and view the status of the Control Policy feature.

What's next

You can create a custom access control policy. For example, you can forbid an operation on a resource in this policy. Then, you can attach this policy to a folder or member in the resource directory to manage the operation permissions of the members on this resource. For more information, see the following topics:

- Create a custom access control policy
- Attach a custom access control policy

5.3. View the details of an access control policy

You can view the name, type, and document of an access control policy, and you can view the folders or members to which the policy is attached.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. On the **Policies** tab, find the access control policy whose details you want to view and click **View** in the **Actions** column.
   - In the **PSP Details** section of the Policy Details page, view **Policy Name**, **Policy Type**, **Policy ID**, **Last Update Time**, and **Policy Description**.
   - On the **Policy JSON** tab, view the document of the policy.
   - On the **Policy Target** tab, view the folders or members to which the policy is attached.

     > **Note** On the **Attachments** tab of the Control Policy page, you can view the access control policies that are attached to each folder or member and the details of each access control policy.

5.4. Disable the Control Policy feature

If you do not want to limit the permissions of folders and members in a resource directory, you can disable the Control Policy feature.

Context

After you disable the Control Policy feature, the system automatically detaches all access control policies that are attached to folders and members. These access control policies are not deleted, but you cannot attach them to folders or members.

> **Note** If you disable the Control Policy feature, the permissions of all folders and members in a resource directory are affected. Proceed with caution.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. In the upper part of the **Control Policy** page, click **Disable Control Policy**.
4. In the message that appears, click **OK**.
5. Click the **Refresh** icon and view the status of the Control Policy feature.

   If the **The control policy feature is disabled** message appears, the Control Policy feature is disabled.

> **Note** If you want to enable the Control Policy feature again, click **Enable Control Policy** in the upper part of the Control Policy page. After you enable the Control Policy feature, the system automatically attaches the default system access control policy FullAliyunAccess to folders and members. You must manually attach custom access control policies to folders or members.

5.5. Languages of access control policies

Before you create or update a custom access control policy, you must understand the basic elements of an access control policy. An access control policy consists of four basic elements: Effect, Action, Resource, and Condition.

Element	Description
Effect	Specifies whether a statement result is an explicit allow or an explicit deny. Valid values: Allow and Deny.
Action	Describes one or more API operations that are allowed or denied.
Resource	Specifies one or more objects that the statement covers.
Condition	Specifies the conditions that are required for a policy to take effect.

Effect

- Valid values are Allow and Deny.

  > **Note** If policies that apply to a request include an Allow statement and a Deny statement, the Deny statement takes precedence over the Allow statement.

- Example: `"Effect": "Allow"`

Action

- Valid values are the names of operations from Alibaba Cloud services. This element can contain one or more values.

  > **Note** In most cases, each Alibaba Cloud service has an exclusive set of API operations. For more information, see the documentation of each Alibaba Cloud service.

- Format: `<ram-code>:<action-name>`.
  - `ram-code`: the code that is used in RAM to indicate an Alibaba Cloud service. For more information, see the codes that are listed in the **RAM code** column in Services that work with RAM.

- `action-name`: the name of one or more API operations in the service.

- Example: `"Action": ["oss:ListBuckets", "ecs:Describe*", "rds:Describe*"]`

> **Note** Microservices Engine (MSE) does not support the Control Policy feature. For more information, see Alibaba Cloud services that do not support the Control Policy feature.

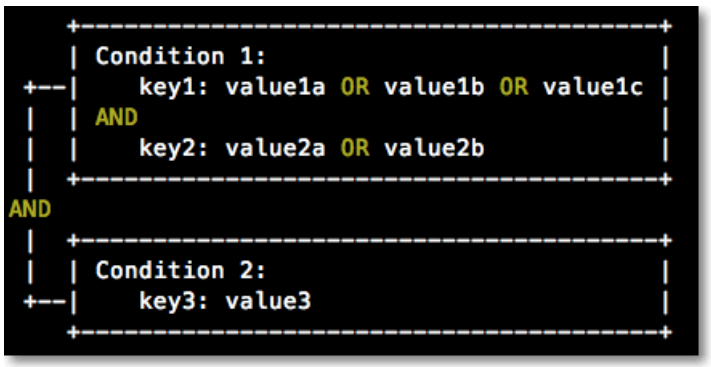
Resource

- Valid values are the Alibaba Cloud Resource Names (ARNs) of the resources. This element can contain one or more values.
- Format: `acs:<ram-code>:<region>:<account-id>:<relative-id>`, which complies with the format of ARNs.
  - `acs`: the acronym of Alibaba Cloud Service.
  - `ram-code`: the code that is used in RAM to indicate an Alibaba Cloud service. For more information, see the codes that are listed in the **RAM code** column in Services that work with RAM.
  - `region`: the information about a region. If the statement covers a global resource, leave this field empty. A global resource can be accessed without the need to specify a region. For more information, see Regions and zones.
  - `account-id`: the ID of the Alibaba Cloud account. For example, you can enter `123456789012***`.
  - `relative-id`: the identifier of the service-related resource. The meaning of this element varies based on services. The format of the relative-id element is similar to a file path. For example, `relative-id = "mybucket/dir1/object1.jpg"` indicates an Object Storage Service (OSS) object.
- Example: `"Resource": ["acs:ecs:*:*:instance/inst-001", "acs:ecs:*:*:instance/inst-002", "acs:oss:*:*:mybucket", "acs:oss:*:*:mybucket/*"]`

> **Note** Microservices Engine (MSE) does not support the Control Policy feature. For more information, see Alibaba Cloud services that do not support the Control Policy feature.

Condition

A condition block contains one or more conditions. Each condition consists of operators, keys, and values.



- Evaluation logic

- You can specify one or more values for a condition key. If the value in a request matches one of the values, the condition is met.
- A condition can have multiple keys that are attached to a single conditional operator. The condition of this type is met only if all requirements for the keys are met.
- A condition block is met only if all of its conditions are met.

- Conditional operators

  Conditional operators can be classified into the following categories: string, number, date and time, Boolean, and IP address.

Category	Conditional operator
String	○ StringEquals ○ StringNotEquals ○ StringEqualsIgnoreCase ○ StringNotEqualsIgnoreCase ○ StringLike ○ StringNotLike
Number	○ NumericEquals ○ NumericNotEquals ○ NumericLessThan ○ NumericLessThanEquals ○ NumericGreaterThan ○ NumericGreaterThanEquals
Date and time	○ DateEquals ○ DateNotEquals ○ DateLessThan ○ DateLessThanEquals ○ DateGreaterThan ○ DateGreaterThanEquals
Boolean	Bool
IP address	○ IpAddress ○ NotIpAddress

- Condition keys
  - The format of common condition keys is `acs:<condition-key>`.

Common condition key	Category	Description

Common condition key	Category	Description
`acs:CurrentTime`	Date and time	The time at which a request is received by the web server. Specify the time in the ISO 8601 format. Example: `2012-11-11T23:59:59Z`.
`acs:SecureTransport`	Boolean	Specifies whether a secure channel is used to send a request. For example, a request can be sent over HTTPS.
`acs:SourceIp`	IP address	The IP address of the client that sends a request. **Note** If you specify only one value for the `acs:SourceIp` condition key, the value must be an IP address, such as 10.0.0.1. CIDR blocks such as 10.0.0.1/32 cannot be used.
`acs:MFAPresent`	Boolean	Specifies whether multi-factor authentication (MFA) is used during user logon.

Common condition key	Category	Description
`acs:PrincipalARN`	String	Specifies the identity of an object that performs an operation. The condition key can be used only in access control policies of resource directories. Example: `acs:ram:*:*:role/*resourcedirectory*`. **Note** You can specify an ARN only for a specified RAM role. The name can contain only lowercase letters. You can view the ARN of a RAM role on the role details page in the RAM console.

- The format of a condition key that is specific to an Alibaba Cloud service is `<ram-code>:<condition-key>`.

Condition key specific to an Alibaba Cloud service	Service	Category	Description
`ecs:tag/<tag-key>`	ECS	String	The tag key of Elastic Compute Service (ECS) resources. This key can be customized. **Note** <tag-key> indicates a tag key. Replace <tag-key> with the actual tag key.

Condition key specific to an Alibaba Cloud service	Service	Category	Description
`rds:ResourceTag/<tag-key>`	RDS	String	The tag key of ApsaraDB RDS resources. This key can be customized. **Note** <tag-key> indicates a tag key. Replace <tag-key> with the actual tag key.
`oss:Delimiter`	OSS	String	The delimiter that is used to categorize OSS object names.
`oss:Prefix`	OSS	String	The prefix of an OSS object name.

References

The syntax and structure of access control policies are similar to those of the permission policies in RAM. For more information, see Policy structure and syntax.

5.6. Manage custom control policies

5.6.1. Create a custom access control policy

You can create a custom access control policy to limit some operations on some resources. Custom access control policies only define permission boundaries for folders and members in a resource directory.

Creation methods

- Create a custom access control policy on the Visual Editor Beta tab

  When you create a custom access control policy on the Visual Editor Beta tab, you need to select configuration items in the Effect, Service, Action, Resource, and Condition sections. In addition, the system can check your configurations to ensure the validity of the policy. On this tab, you can perform simple operations to create a custom access control policy.

- Create a custom access control policy on the JSON tab

  When you create a custom access control policy on the JSON tab, you must compile the document of the policy based on the syntax and structure of access control policies. On this tab, you can create a custom access control policy in a flexible manner. This method is suitable for users who are familiar with the syntax and structure of access control policies.

Create a custom access control policy on the Visual Editor Beta tab

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. On the **Policies** tab of the page that appears, click **Create Policy**.
4. On the **Create Policy** page, click the **Visual Editor Beta** tab.
5. Configure the policy and click **Next: Edit Basic Information**.
   i. In the **Effect** section, select **Allow** or **Deny**.
   ii. In the **Service** section, select an Alibaba Cloud service.

   > **Note** All supported Alibaba Cloud services are displayed in the Service section.

   iii. In the **Action** section, select **All Actions** or **Specified Actions**.

   The system displays the actions that can be configured based on the Alibaba Cloud service that you select in the Service section. If you select **Specified Actions**, you must select specific actions.

   iv. In the **Resource** section, select **All Resources** or **Specified Resources**.

   The system displays the resources that can be configured based on the actions that you select in the Action section. If you select **Specified Resources**, you must click **Add Resource** to configure the Alibaba Cloud Resource Names (ARNs) of resources. You can also select **Match All** to specify all resources for each selected action.

   > **Note** The resource ARNs that are required for an action are tagged with **Required**. We strongly recommend that you configure the resource ARNs that are tagged with Required. This ensures that the policy takes effect as expected.

   v. (Optional)In the **Condition** section, click **Add Condition** to configure conditions.

   Conditions include Alibaba Cloud common conditions and service-specific conditions. The system displays the conditions that can be configured based on the Alibaba Cloud service and the actions that you select. You need only to select condition keys and configure the Operator and Value parameters for each condition key.

   vi. Click **Add Statement** and repeat the preceding steps to configure multiple statements for the policy.
6. Configure the **Name** and **Note** parameters.
7. Check and optimize the policy document.
   - Basic optimization

     The system performs the following operations during basic optimization:

     - Deletes unnecessary conditions.
     - Deletes unnecessary arrays.
   - (Optional)Advanced optimization

     You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. Then, the system performs the following operations during advanced optimization:

     - Splits resources or conditions that are incompatible with actions.

- Narrows down resources.
- Deduplicates or merges policy statements.

8. Click **OK**.

Create a custom access control policy on the JSON tab

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. On the **Policies** tab of the page that appears, click **Create Policy**.
4. On the **Create Policy** page, click the **JSON** tab.
5. Enter the policy document and click **Next: Edit Basic Information**.

   For more information about the syntax and structure of access control policies, see Languages of access control policies.
6. Configure the **Name** and **Note** parameters.
7. Check and optimize the policy document.
   - Basic optimization

     The system performs the following operations during basic optimization:
     - Deletes unnecessary conditions.
     - Deletes unnecessary arrays.
   - (Optional)Advanced optimization

     You can move the pointer over **Optional: Advanced Optimize** and click **Perform**. Then, the system performs the following operations during advanced optimization:
     - Splits resources or conditions that are incompatible with actions.
     - Narrows down resources.
     - Deduplicates or merges policy statements.

What's next

After a custom access control policy is created, you must attach it to folders or members for it to take effect. For more information, see Attach a custom access control policy.

5.6.2. Modify a custom access control policy

You can modify the name, description, and document of a custom access control policy based on your business requirements. If you modify the document of a custom access control policy, the modification immediately takes effect on the folders or members to which the policy is attached.

Context

A system access control policy cannot be modified.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.

3. On the **Policies** tab of the page that appears, click the name of the custom access control policy that you want to modify.
4. On the **Policy Details** page, click **Modify Policy** in the upper-right corner.
5. On the Visual Editor Beta or JSON tab, modify the document of the policy and click **Next: Edit Basic Information**.

   For more information, see Create a custom access control policy.
6. Change the values of **Name** and **Note** and click **OK**.

5.6.3. Delete a custom access control policy

You can delete a custom access control policy that is not attached to folders or members.

Context

- System access control policies cannot be deleted.
- If you want to delete a custom access control policy that is attached to folders or members, you must detach this policy from the folders or members first. Then, you can delete this policy. For more information, see Detach a custom access control policy.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. On the **Policies** tab, find the custom access control policy that you want to delete and click **Delete** in the **Actions** column.
4. In the message that appears, click **OK**.

5.6.4. Attach a custom access control policy

You can attach a custom access control policy to folders or members. After you attach a custom access control policy, the operations performed on resources by using members are limited by the policy. Make sure that the attached policy meets your expectations. Otherwise, your business may be affected.

Context

- By default, the system access control policy **FullAliyunAccess** is attached to each folder and member.
- The access control policy that is attached to a folder also applies to all its subfolders and all members in the subfolders.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. On the Control Policy page, click the **Attachments** tab. In the navigation tree of the Attachments tab, find the folder or member to which you want to attach an access control policy. Then, click the name of the folder or member.
4. In the section that appears, click **Attach Policy**.

5. In the **Attach Policy** dialog box, select the access control policy that you want to attach to the folder or member.
6. Click **OK**.

5.6.5. Detach a custom access control policy

If you no longer need a custom access control policy, you can detach it from the related folders or members. After you detach it, the custom access control policy no longer limits the operations that are performed on resources by members.

Context

The system access control policy FullAliyunAccess is attached to each folder and member by default and cannot be detached from them.

Procedure

1. Log on to the Resource Management console.
2. In the left-side navigation pane, choose **Resource Directory > Control Policy**.
3. On the Control Policy page, click the **Attachments** tab. In the navigation tree of the tab, find the folder or member from which you want to detach a custom access control policy. Then, click the name of the folder or member.
4. In the section that appears, find the custom access control policy that you want to detach and click **Detach** in the **Actions** column.
5. In the message that appears, click **OK**.

5.6.6. Examples of custom access control policies

This topic describes examples of custom access control policies.

Overview

- Policy 1: You are not allowed to modify or delete RAM users, RAM user groups, or RAM roles
- Policy 2: You are not allowed to modify the role ResourceDirectoryAccountAccessRole or change its permissions
- Policy 3: You are not allowed to modify or delete the specified RAM users
- Policy 4: You are not allowed to enable logon to the Alibaba Cloud Management Console for an existing RAM user
- Policy 5: You must complete MFA when you use a RAM user or RAM role to delete some resources
- Policy 6: You are not allowed to modify user-based SSO settings
- Policy 7: You are not allowed to modify role-based SSO settings
- Policy 8: You are not allowed to disable the Delivery feature of ActionTrail or change the destination to which ActionTrail delivers events
- Policy 9: You are not allowed to access some network services
- Policy 10: You are not allowed to create network resources (EIPs and NAT gateways) that can be used to access the Internet
- Policy 11: You are not allowed to access network services that are connected to on-premises resources

Policy 1: You are not allowed to modify or delete RAM users, RAM user groups, or RAM roles

Document:

```
{
    "Statement": [
        {
            "Action": [
                "ram:Attach*",
                "ram:Detach*",
                "ram:BindMFADevice",
                "ram:CreateAccessKey",
                "ram:CreateLoginProfile",
                "ram:CreatePolicyVersion",
                "ram:DeleteAccessKey",
                "ram:DeleteGroup",
                "ram:DeleteLoginProfile",
                "ram:DeletePolicy",
                "ram:DeletePolicyVersion",
                "ram:DeleteRole",
                "ram:DeleteUser",
                "ram:DisableVirtualMFA",
                "ram:AddUserToGroup",
                "ram:RemoveUserFromGroup",
                "ram:SetDefaultPolicyVersion",
                "ram:UnbindMFADevice",
                "ram:UpdateAccessKey",
                "ram:UpdateGroup",
                "ram:UpdateLoginProfile",
                "ram:UpdateRole",
                "ram:UpdateUser"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN":"acs:ram:*:*:role/resourcedirectoryaccountaccessrole
"
                }
            }
        }
    ],
    "Version": "1"
}
```

The preceding policy defines that you are not allowed to modify or delete RAM users, RAM user groups, or RAM roles, including their permissions.

Note In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 2: You are not allowed to modify the role ResourceDirectoryAccountAccessRole or change its permissions

Document:

```
{
   "Version": "1",
   "Statement": [
       {
           "Effect": "Deny",
           "Action": [
               "ram:UpdateRole",
               "ram:DeleteRole",
               "ram:AttachPolicyToRole",
               "ram:DetachPolicyFromRole"
           ],
           "Resource": "acs:ram:*:*:role/resourcedirectoryaccountaccessrole"
       }
   ]
}
```

Policy 3: You are not allowed to modify or delete the specified RAM users

Document:

```
{
    "Version": "1",
    "Statement": [{
        "Action": [
            "ram:AttachPolicyToUser",
            "ram:DetachPolicyFromUser",
            "ram:AddUserToGroup",
            "ram:RemoveUserFromGroup",
            "ram:UpdateUser",
            "ram:DeleteUser",
            "ram:CreateLoginProfile",
            "ram:UpdateLoginProfile",
            "ram:DeleteLoginProfile",
            "ram:CreateAccessKey",
            "ram:DeleteAccessKey",
            "ram:UpdateAccessKey",
            "ram:BindMFADevice",
            "ram:UnbindMFADevice",
            "ram:DisableVirtualMFA"
        ],
        "Resource": [
            "acs:ram:*:*:user/Alice"
        ],
        "Effect": "Deny",
        "Condition": {
            "StringNotLike": {
                "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrole"
            }
        }
    }]
}
```

The preceding policy defines that you are not allowed to modify or delete the specified RAM users, including their permissions. For example, if a RAM user Alice exists, you cannot perform the preceding operations on Alice. You can specify the Alibaba Cloud account to which Alice belongs, such as `acs:ram:*:18299873****:user/Alice`.

> **Note** In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 4: You are not allowed to enable logon to the Alibaba Cloud Management Console for an existing RAM user

Document:

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateLoginProfile",
                "ram:UpdateLoginProfile"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

The preceding policy defines that you are not allowed to enable logon to the Alibaba Cloud Management Console for an existing RAM user. You can still enable logon to the Alibaba Cloud Management Console for a new RAM user.

> **Note** In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 5: You must complete MFA when you use a RAM user or RAM role to delete some resources

Document:

```
{
  "Statement": [
    {
      "Action": "ecs:DeleteInstance",
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Bool": {
          "acs:MFAPresent": "false"
        }
      }
    }
  ],
  "Version": "1"
}
```

The preceding policy defines that you must complete multi-factor authentication (MFA) when you use a RAM user or RAM role to delete Elastic Compute Service (ECS) instances. If you want to delete other resources, change the value of Action to the action for the resources.

Policy 6: You are not allowed to modify user-based SSO settings

Document:

```
{
    "Statement": [
        {
            "Action": [
                "ram:SetSamlSsoSettings"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

Note In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 7: You are not allowed to modify role-based SSO settings

Document:

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateSAMLProvider",
                "ram:DeleteSAMLProvider",
                "ram:UpdateSAMLProvider"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

Note In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 8: You are not allowed to disable the Delivery feature of ActionTrail or change the destination to which ActionTrail delivers events

Document:

```
{
    "Statement": [
        {
            "Action": [
                "actiontrail:UpdateTrail",
                "actiontrail:DeleteTrail",
                "actiontrail:StopLogging"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

Note In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 9: You are not allowed to access some network services

Document:

```
{
    "Statement": [
        {
            "Action": [
                "vpc:*HaVip*",
                "vpc:*RouteTable*",
                "vpc:*VRouter*",
                "vpc:*RouteEntry*",
                "vpc:*VSwitch*",
                "vpc:*Vpc*",
                "vpc:*Cen*",
                "vpc:*NetworkAcl*"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        },
        {
            "Action": [
                "vpc:*VpnGateway*",
                "vpc:*VpnConnection*",
                "vpc:*CustomerGateway*",
                "vpc:*SslVpnServer*",
                "vpc:*SslVpnClientCert*",
                "vpc:*VpnRoute*",
                "vpc:*VpnPbrRoute*"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

The preceding policy defines that you are not allowed to access Virtual Private Cloud (VPC) and VPN Gateway. If you want to deny access to other network services, change the value of Action to the action for these network services.

> **Note** In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 10: You are not allowed to create network resources (EIPs and NAT gateways) that can be used to access the Internet

Document:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "vpc:AllocateEipAddress",
                "vpc:AllocateEipAddressPro",
                "vpc:AllocateEipSegmentAddress",
                "vpc:CreateNatGateway"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ]
}
```

> **Note** In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 11: You are not allowed to access network services that are connected to on-premises resources

Document:

```
{
    "Statement": [
       {
            "Action": [
                "vpc:*PhysicalConnection*",
                "vpc:*VirtualBorderRouter*",
                "cen:*",
                "vpc:*VpnGateway*",
                "vpc:*VpnConnection*",
                "vpc:*CustomerGateway*",
                "vpc:*SslVpnServer*",
                "vpc:*SslVpnClientCert*",
                "vpc:*VpnRoute*",
                "vpc:*VpnPbrRoute*",
                "smartag:*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ],
    "Version": "1"
}
```

The preceding policy defines that you are not allowed to access network services that are connected to on-premises resources. These network services include Express Connect, Cloud Enterprise Network, VPN Gateway, and Smart Access Gateway.

Policy 12: You are not allowed to use some features provided by Billing Management

Document:

```
{
    "Statement": [
       {
            "Action": [
                "bss:DescribeOrderList",
                "bss:DescribeOrderDetail",
                "bss:PayOrder",
                "bss:CancelOrder"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ],
    "Version": "1"
}
```

The preceding policy defines that you are not allowed to use the Orders feature provided by Billing Management. If you want to prohibit the use of other features, change the value of Action to the action for these features.

> **Note** In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 13: You are not allowed to modify the settings of CloudMonitor

Document:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "cms:Put*",
                "cms:Update*",
                "cms:Create*",
                "cms:Modify*",
                "cms:Disable*",
                "cms:Enable*",
                "cms:Delete*",
                "cms:Send*",
                "cms:Subscribe*",
                "cms:Unsubscribe*",
                "cms:Remove*",
                "cms:CreateAction",
                "cms:Pause*",
                "cms:Stop*",
                "cms:Start*",
                "cms:BatchCreate*",
                "cms:ProfileSet",
                "cms:ApplyMonitoringTemplate"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "acs:PrincipalARN": "acs:ram:*:*:role/resourcedirectoryaccountaccessrol
e"
                }
            }
        }
    ]
}
```

Note In this policy, only ResourceDirectoryAccountAccessRole, which is the default role used to access members in a resource directory, can be used to perform the preceding operations. You can remove this condition to make sure that all RAM users and RAM roles cannot be used to perform these operations. You can also specify RAM users or RAM roles that can be used to perform the operations by changing the value of PrincipalARN.

Policy 14: You are not allowed to purchase reserved instances

Document:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:PurchaseReservedInstancesOffering"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

Policy 15: You are not allowed to create ECS instances in an unspecified VPC

Document:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:CreateInstance",
                "ecs:RunInstances"
            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "StringNotLike": {
                    "vpc:VPC": "acs:vpc:cn-shenzhen:*:vpc/vpc-wz95ya85js0avrkabc****"
                }
            }
        }
    ]
}
```

In the preceding policy, acs:vpc:cn-shenzhen:*:vpc/vpc-wz95ya85js0avrkabc**** is used as a specified VPC. You can replace it based on your business requirements.

Policy 16: You are not allowed to purchase domain names

Document:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "domain:CreateOrderActivate"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

Policy 17: You are not allowed to access the Support and Services console

Document:

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "support:*",
                "workorder:*"
            ],
            "Resource": "*",
            "Effect": "Deny"
        }
    ]
}
```

Policy 18: You are not allowed to access ECS in a specific region

Document:

```
{
    "Version": "1",
    "Statement": [{
        "Effect": "Deny",
        "Action": [
            "ecs:*"
        ],
        "Resource": "acs:ecs:us-east-1:*:*"
    }]
}
```

The preceding policy defines that you are not allowed to access ECS in the US (Virginia) region.

6.Manage trusted services

6.1. Overview

Trusted services refer to the Alibaba Cloud services that are integrated with the Resource Directory service. After an Alibaba Cloud service is integrated with Resource Directory, the service can access the information of the related resource directory, such as the members and folders in the resource directory. You can use the management account of your resource directory or a delegated administrator account of a trusted service to manage your business in the trusted service based on your resource directory. This simplifies the unified management of cloud services activated by your enterprise. For example, after Cloud Config is integrated with Resource Directory, you can use the management account of your resource directory to view related information in Cloud Config. The information includes the resources of all members in the resource directory, as well as the configuration history and compliance statuses of the resources. You can also monitor the compliance of resource configurations in Cloud Config.

Use a trusted service

Trusted services can be used by calling API operations or by using their consoles. This section describes how to use a trusted service in its console.

1. Log on to the Resource Management console by using an Alibaba Cloud account and enable a resource directory. This Alibaba Cloud account is the management account of the resource directory.

   For more information, see Enable a resource directory.

2. In the Resource Management console, build an organizational structure for your enterprise. You can create members in the resource directory or invite existing Alibaba Cloud accounts to join the resource directory.

   For more information, see Create a folder, Create a member, and Invite an Alibaba Cloud account to join a resource directory.

3. Optional. In the Resource Management console, specify a member as a delegated administrator account of the trusted service.

   If you do not specify a delegated administrator account for the trusted service, you can use only the management account to manage your business in the trusted service.

   For more information about how to specify a delegated administrator account for a trusted service, see Add a delegated administrator account.

   > **Note** This step applies only to trusted services that support delegated administrator accounts.

4. In the console of the trusted service, use the management account or delegated administrator account to enable the multi-account management feature. Then, select the members that you want to manage in a unified manner based on the organizational structure of your resource directory, and manage the operations on the selected members.

   This step varies based on the specific trusted service. For more information, see the References column in the Supported trusted services section.

Supported trusted services

Trusted service	Description	Support for delegated administrator accounts	References
Cloud Config	After Cloud Config is integrated with Resource Directory, you can use the management account of your resource directory to view related information in Cloud Config. The information includes the resources of all the members in the resource directory, as well as the configuration history and compliance statuses of the resources. You can also monitor the compliance of resource configurations in Cloud Config.	Yes	Account group overview
ActionTrail	After ActionTrail is integrated with Resource Directory, you can use the management account of your resource directory to create multi-account trails in ActionTrail. A multi-account trail delivers the events of all members in a resource directory to an Object Storage Service (OSS) bucket or a Log Service Logstore.	Yes	Multi-account trail overview
Security Center	After Security Center is integrated with Resource Directory, Security Center provides an interface that displays security risks detected for all the members in your resource directory.	Yes	Use the multi-account control feature

Trusted service	Description	Support for delegated administrator accounts	References
Cloud Firewall	After Cloud Firewall is integrated with Resource Directory, you can use Cloud Firewall to centrally manage the public IP addresses of the resources within multiple accounts. You can also configure defense policies for the public IP addresses and view log analysis results in a unified manner. This implements centralized security control.	Yes	Use centralized account management
Dynamic Route for CDN (DCDN)	After DCDN is integrated with Resource Directory, DCDN can provide the multi-account management feature and unify the management of domain names that belong to different accounts and products.	No	None
CloudMonitor	After CloudMonitor is integrated with Resource Directory, CloudMonitor can monitor the resources within multiple Alibaba Cloud accounts used by your enterprise in a centralized manner.	Yes	Overview of Hybrid Cloud Monitoring

Trusted service	Description	Support for delegated administrator accounts	References
CloudSSO	After CloudSSO is integrated with Resource Directory, you can use the management account of your resource directory to centrally manage the accounts of users who use Alibaba Cloud services in your enterprise in CloudSSO. You can configure single sign-on (SSO) between your enterprise identity management system and Alibaba Cloud. In addition, you can configure access permissions for users on the members of your resource directory in a centralized manner.	No	Overview
Log Audit Service	After Log Audit Service is integrated with Resource Directory, Log Audit Service can automatically collect the logs of Alibaba Cloud services from multiple accounts, and store, audit, and analyze the logs in a centralized manner.	Yes	Configure multi-account collection
Resource Orchestration Service (ROS)	After ROS is integrated with Resource Directory, you can use the management account of your resource directory to deploy the resources that are required by your system within the members of the resource directory. This achieves centralized resource management in a multi-account environment.	Yes	Stack group overview

Trusted service	Description	Support for delegated administrator accounts	References
Resource Sharing	After resource sharing is enabled, you can use the management account of your resource directory to share your resources with all members in your resource directory, all members in a specific folder in your resource directory, or a specific member in your resource directory. For members that are newly added to your resource directory, the system automatically grants access permissions on shared resources to the members based on your resource sharing settings. For members that are removed from your resource directory, the system automatically revokes access permissions on shared resources from the members if the members have such permissions.	No	Resource Sharing overview
Cloud Governance Center	After Cloud Governance Center is integrated with Resource Directory, you can view the distribution and change status of the resources within the members of your resource directory in the Cloud Governance Center console. You can also configure protection rules for the compliance audit and deliver audit logs for the members in a unified manner.	No	• Deliver audit logs in a unified manner • Configure protection rules in a centralized manner • View resource distribution and the trend in resource quantity

Trusted service	Description	Support for delegated administrator accounts	References
Tag	You can use the management account of your resource directory to enable the Tag Policy feature that is in multi-account mode. Then, you can use tag policies to manage the tag-related operations performed by using a member within the resource directory.	No	Enable the Tag Policy feature that is in multi-account mode

Enable or disable a trusted service

You can enable or disable a trusted service by using the console or API of the service. For more information, see the documentation of the service.

You can choose **Resource Directory > Trusted Services** in the left-side navigation pane of the Resource Management console to view the statuses of trusted services. You cannot enable or disable trusted services in the Resource Management console.

When you use some trusted services to perform specific operations, Resource Directory automatically updates the states of the trusted services to Enabled. For example, if you create a multi-account trail in ActionTrail or use a trusted service to view the resources related to Resource Directory for the first time, Resource Directory automatically updates the state of ActionTrail or the trusted service to Enabled.

When you use some trusted services to perform specific operations, Resource Directory automatically updates the states of the trusted services to Disabled. For example, if you disable a feature provided by a trusted service, Resource Directory automatically updates the state of the trusted service to Disabled. If a trusted service is disabled, the service cannot access the members or resources in your resource directory. In addition, the resources that are related to integration with Resource Directory are deleted from the trusted service.

Service-linked roles for trusted services

Resource Directory creates its service-linked role AliyunServiceRoleForResourceDirectory for each member. This role enables Resource Directory to create the roles required by trusted services. Only Resource Directory can assume this role. For more information, see Service-linked role for Resource Directory.

Trusted services create their own service-linked roles, such as the AliyunServiceRoleForConfig role of Cloud Config, only for the members that are used to perform administrative operations. These roles define the permissions required by trusted services to perform specific tasks. Only trusted services can assume their own service-linked roles.

The policy that is attached to a service-linked role is defined and used by the linked service. You are not allowed to modify or delete the policy. In addition, you are not allowed to attach policies to or detach policies from a service-linked role. For more information, see Service-linked roles.

6.2. Manage a delegated administrator account

This topic provides the definition and limits of a delegated administrator account and describes how to manage a delegated administrator account.

What is a delegated administrator account?

The management account of a resource directory can be used to specify a member in the resource directory as a delegated administrator account of a trusted service. After a member is specified as a delegated administrator account of a trusted service, the member can be used to access the information of the resource directory in the trusted service. The information includes the structure and members of the resource directory. The member can also be used to manage business within the resource directory. For more information, see Trusted services that support delegated administrator accounts.

Delegated administrator accounts allow you to separate organization management tasks from business management tasks. The management account of a resource directory is used to perform the organization management tasks of the resource directory. Delegated administrator accounts are used to perform the business management tasks of the related trusted services. This meets security-related requirements.

Limits

- Only some trusted services support delegated administrator accounts. For more information, see Supported trusted services.
- Only the management account of a resource directory or its RAM user or RAM role that has the permissions specified in the following code can be used to add or remove delegated administrator accounts:

```
{
    "Version": "1",
    "Statement": [{
        "Action": [
            "resourcemanager:RegisterDelegatedAdministrator",
            "resourcemanager:DeregisterDelegatedAdministrator"
        ],
        "Resource": "*",
        "Effect": "Allow"
    }]
}
```

  For more information about how to create a custom policy, see Create a custom policy.

- Delegated administrator accounts can only be the members of a resource directory. The management account of a resource directory cannot be specified as a delegated administrator account.
- The number of delegated administrator accounts that are allowed for a trusted service is defined by the trusted service.

Add a delegated administrator account

1. Log on to the Resource Management console by using the management account of your resource directory.
2. In the left-side navigation pane, choose **Resource Directory > Trusted Services**.
3. On the **Trusted Services** page, find the trusted service for which you want to add a delegated administrator account, and click **Manage** in the **Actions** column.
4. In the **Delegated Administrator Accounts** section of the page that appears, click **Add**.
5. In the **Add Delegated Administrator Account** panel, select a member.
6. Click **OK**.
   Then, you can use the delegated administrator account to access the multi-account management module of the trusted service and perform administrative operations within the resource directory.

Remove a delegated administrator account

Notice The removal of a delegated administrator account may affect the use of the related trusted service. Proceed with caution when you perform this operation.

1. Log on to the Resource Management console by using the management account of your resource directory.
2. In the left-side navigation pane, choose **Resource Directory > Trusted Services**.
3. On the **Trusted Services** page, find the trusted service for which you want to remove a delegated administrator account, and click **Manage** in the **Actions** column.
4. In the **Delegated Administrator Accounts** section of the page that appears, find the delegated administrator account that you want to remove, and click **Remove** in the **Actions** column.
5. In the **Warning** message, click **Continue**.
   Then, the account can no longer be used to access the information of the resource directory and view the structure and members of the resource directory in the trusted service.