Alibaba Cloud
Resource Access Management

User Guide

Issue: 20190218

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
`Italics`	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich {stand | slave}`

Contents

1 Overview

This topic describes the core functions of RAM and their typical scenarios.

Core functions

Identity management

- *Users*
- *User groups*
- *Federated SSO overview*
- *Configure the SAML of an external IdP*
- *Example*
- *Manage RAM roles*

Authorization management

- *Policy management*
- *Permission granting in RAM*
- *Permission check rules*

Typical scenarios

- *User management and access control*
- *Temporary authorization for mobile apps*
- *Cross-account resource authorization and access*
- *Dynamic identity and permission management of cloud applications*
- *Use a local enterprise account to log on to Alibaba Cloud*

2 Identity management

2.1 User management

2.1.1 Users

A RAM user is a type of identity used in RAM. It represents an entity, for example, a person or an application. If a new user or an application wants to access your Alibaba Cloud resources, you must create a RAM user and grant it relevant permissions to access the resources.

The general procedure is as follows:

1. Log on to the *RAM console* using your Alibaba Cloud account credentials (or the credentials of a relevant RAM user account).
2. Create a RAM user and select an access mode: You can select console password logon or programmatic access.
3. Grant permissions to the RAM user: You can add the RAM user to one or more user groups or attach one or more policies to it as required.

Create a RAM user

1. In the RAM console, select Identities > Users > Create User.
2. Enter a logon name and a display name for the user. To create multiple RAM users at a time, click Add User.
3. Select Console Password Logon or Programmatic Access as the access mode.

   Note:
   We recommend that you select only one access mode for the RAM user.

   - If you select Console Password Logon, you must also complete the basic security settings for logon, including deciding whether to automatically generate a password or customize the logon password, setting whether the user must reset the password upon the next logon, and setting whether to enable Multi-Factor Authentication (MFA).
   - If you select Programmatic Access, an AccessKey (API access key) is automatically created for the user.

Grant permissions to a RAM user

After creating a RAM user, you can click Add Permissions to grant it permissions.

1. From the list of created users, select the target user.
2. Click Add Permissions. On the displayed Add Permissions page, the principal is entered automatically.
3. Select the policy that you want to attach to the RAM user and then click OK.

Manage a RAM user

After creating a RAM user, you can manage and change the user settings as needed.

- Edit basic user information

  1. In the RAM console, click Users, locate your target user, and click the user name.

     
     Note:
     You can enter keywords to search for a specific user name.

  2. In the Basic Information area, click Modify Basic Information.
  3. On the displayed Modify Basic Information page, you can change the user display name, add helpful remarks.

- Manage console logon

  You can set a logon password for users to use when they log on to the console.

  1. In the RAM console, click Users, locate your target user, and click the user name.

     
     Note:
     You can enter keywords to search for a specific user name.

  2. In the Console Logon Management area, click Modify Logon Settings.
  3. On the Modify Logon Settings page, modify the logon settings for the user.

     The logon settings include:

     - Decide whether to enable console password logon.
     - Set the logon password.
     - Decide whether the user must reset the password upon the next logon.
     - Decide whether to enable MFA.

- Enable MFA

  MFA is a simple but effective best practice that can provide additional security protection compared with traditional user name and password method.

  1. Make sure that you have selected Required for Enable MFA when you Modify Logon Settings through Console Logon Management.
  2. After the user logs on to the console as a RAM user, the MFA device binding process is prompted. The user can follow the process to complete the MFA device binding.

  After you enable MFA, two authentication factors are required when the user logs on to Alibaba Cloud:

  - The first authentication factor is a user name and password combination.
  - The second authentication factor is a code generated by the MFA device as specified by the user.

  The specified MFA device is an application that generates a 6-digit verification code that complies with the time-based one-time password algorithm (TOTP) standard *RFC 6238*. Such an application is generally an app that runs on a target mobile device (such as Google Authenticator).

- Manage AccessKeys

  Create an AccessKey

  To create an AccessKey (AK) for a user who needs to call APIs, follow these steps:

  1. In the RAM console, click Users, locate the target user, and click the user name.

     Note:
     You can enter keywords to search for a specific user name.

  2. In the Access Keys area, click Create AccessKey.
  3. In the displayed dialog box, confirm the AK information and save it in time.

     Note:

     - The AK information is displayed one time only during its initial creation.
     - For security reasons, RAM does not provide an AK query interface.

- If the AK is mistakenly disclosed or lost, you must create a new one.

Disable an AK

You can disable or enable an AK in the Access Keys area.

Delete an AK

 Notice:
Do not delete an AK if it is being used by another user. Deleting an AK that is currently in use may cause service failure. Exercise caution when performing this action.

To confirm the usage status of an AK, check the timestamp through Last Used in the Access Keys area.

Log on to the console as a RAM user

Logon portal

To maintain account security, the logon portal for RAM users is different from that of the Alibaba Cloud account.

The RAM user's logon link is *https://signin.aliyun.com/aliyun-document.onaliyun.com/login.htmhttps://signin-intl.aliyun.com/testzzx-intl.onaliyun.com/login.htm* . (You can also find the logon link on the Overview page after you log on to the *RAM console*.)

Logon information

The RAM user logon account is in User Principal Name (UPN) format and the full account format is <$username>@<$AccountAlias>.onaliyun.com, which is the user logon name shown in the user list in the RAM console.

On the RAM user logon page, users can log on using the UPN format or <$username>@<$AccountAlias>.

- Each Alibaba Cloud account has a Default Domain. To view or modify the domain name, log on to the RAM console, go to the Identities page, and select Settings > Advanced.
  - The format of the Default Domain is <$AccountAlias>.onaliyun.com.
  - If you have not set any account alias, the account alias is set to the AccountID by default, and the Default Domain is in the following format: <$AccountID>.onaliyun.com.

- You can also configure a Domain Alias for your account and the RAM user can use the domain alias to log on. To view the domain alias, log on to the RAM console, go to the Identities page, and click Settings > Advanced.

  For more information about Domain Alias, see *Configure the SAML of an account*.

> Note:
> By default, RAM users do not have any access permissions. A RAM user without permissions can log on to the console, but cannot perform any operations. For more information about how to grant RAM users permissions, see *Permission granting in RAM*.

Delete a RAM user

> Notice:
> Do not delete a RAM user that is active. Deleting an active RAM user may result in service failure. Exercise caution when performing this action.

1. In the RAM console, click Users. Then, locate the RAM user that you want to delete.
2. Click Delete.
3. In the displayed Delete User dialog box, click OK.

2.1.2 User groups

If you have created multiple RAM users under your account, you can create user groups to classify and organize these RAM users for easier user and permission management.

Adding RAM users to user groups means that:

- When the responsibilities of a user change, you only need to move this user to a group that has the appropriate permissions. Other RAM users are not affected.
- When the responsibilities of a user group change, you only need to modify the policy attached to the group, and all changes to the policy apply to all RAM users in the group.

Create a user group

1. In the *RAM console*, click Identities > Groups > Create Group.
2. Enter a group name, a display name, and a note for the group and click OK.

Manage group members

1. In the RAM console, click Groups. Then, locate the target group and click the group name.

    Note:
   Fuzzy search is supported for user group names.

2. Click the Group Members tab to manage group members.
   - Add group members: Click Add Group Members. On the displayed Add Group Members page, select the users you want to add to the group (or enter keywords to search) from the left column, and then click OK.

      Note:
     You can click "×" to clear your selection.

   - Remove group members: To remove a member from a group, find the user that you want to remove and click Remove from Group.

Rename a user group

1. In the RAM console, click Groups. Then, locate the group that you want to rename and click the group name.

    Note:
   Fuzzy search is supported for user group names.

2. Click Modify Basic Information.
3. Enter a display name and click OK.

Delete a user group

1. In the RAM console, click Groups and locate the group that you want to delete.

    Note:
   Fuzzy search is supported for user group names.

2. Click Delete.
3. In the displayed Delete Group dialog box, click OK.

    Note:

If the group contains any members or is attached to any policies, these members and policies will be removed from the group.

Grant permissions to a user group

For more information about how to grant permissions to a group, see *Permission granting in RAM*.

2.2 Logon security settings

2.2.1 Security settings

You can define the logon password requirements and set the access mode for RAM users through security settings.

Logon password settings

1. In the *RAM console*, click Identities > Settings.
2. On the Security Settings tab page, click Edit Password Rule.
3. Define such rules as Password Length, Required Elements in Password, Password Validity Period, and Password Retry Constraint Policy, and then click OK.

Note:
After you complete the settings, these settings apply to all RAM users.

User security settings

1. In the RAM console, click Identities > Settings.
2. On the Security Settings tab page, click Update RAM user security settings.
3. Modify the required settings and then click OK.

2.2.2 域名管理

每个云账号有默认域名，除了默认域名，也可为账号配置域别名。RAM 用户可以通过默认域名或域别名登录，通过域名管理可以修改登录名后缀，便于用户记忆登录名称。

RAM 用户登录的前提条件

RAM 用户登录账号为 UPN (User Principal Name) 格式，即 RAM 控制台用户列表中所见的用户登录名称。

在 RAM 用户登录入口，用户可以两种使方式登录：

- UPN 完整格式<$username>@<$AccountAlias>.onaliyun.com。

- <$username>@<$AccountAlias>。

RAM 用户登录入口

RAM 用户和云账号的登录入口不同，RAM 用户不能通过云账户登录页面进行登录。

RAM 用户的登录入口如下：*https://signin.alibabacloud.com/login.htm*。

> Note:
> 通过登录 *RAM* 控制台，在概览页可以快速查询登录链接。

域名管理

默认域名

1. 登录 RAM 控制台。
2. 在人员管理菜单下，单击设置 > 高级设置可以查询和修改默认域名。
   - 默认域名的格式为: <$AccountAlias>.onaliyun.com。
   - 若未设置过账号别名，账号别名默认值为 AccountID，此时默认域名的格式为：<$AccountID>.onaliyun.com。

域别名

除了默认域名，也可为账号配置域别名，RAM 用户同样可使用域别名登录。

1. 登录 RAM 控制台。
2. 在人员管理菜单下，单击设置 > 高级设置可以查询域别名。
3. 单击创建域别名。
4. 填写域名。
5. 单击确定。
6. 进行域名归属验证。

> Note:
> 创建域别名成功后，复制弹出的随机验证码，到域名购买平台进行域名解析 TXT 记录设置；设置完毕后，再进行域名归属验证。

更多信息

关于创建域别名及单点登录设置，请参考联合登录概述。

具体的域别名操作方式，请参考云账号的 *SAML* 设置。

2.3 Identity federation management

2.3.1 Federated SSO overview

Many enterprises want to leverage their own identity systems, including those from other providers, to enable federated Single Sign On (SSO) to better manage their resources and applications deployed locally and in the cloud. This topic describes Alibaba Cloud RAM federated SSO solution to help users quickly understand and configure federated SSO.

Alibaba Cloud supports the *SAML 2.0 (Security Assertion Markup Language 2.0)* Identity Federation open standards that are widely used by enterprise identity providers (IdPs). By enabling federated SSO, users can use the account authentication mechanism of their organization to log on to the Alibaba Cloud console.

The following table details some basic terms related to SAML federated SSO.

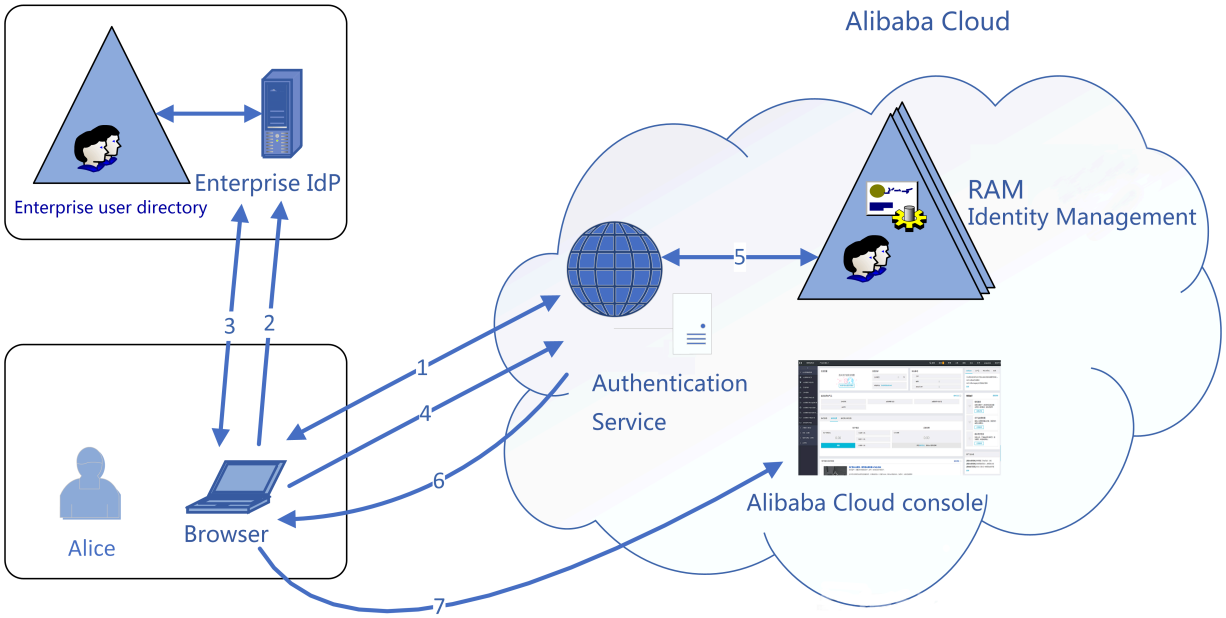
Terms

Term	Description
Identity Provider (IdP)	Provides identity management services, for example: · Locally deployed IdPs, such as Microsoft Active Directory Federation Service (AD FS) and Shibboleth. · Cloud-based IdPs, such as Azure AD, Google G Suite, Okta, and OneLogin.
Service Provider (SP)	Uses the identity management function of an IdP to provide users with specific service applications. An SP uses the user information provided by an IdP. In some identity systems (such as OpenID Connect) that do not comply with the SAML protocol, Service Provider is known as Relying Party, which means the relying party of an IdP.
Security Assertion Markup Language (SAML)	A standard protocol for enterprise-level user identity authentication. It can be used to achieve communication between an SP and an IdP. SAML 2.0 is a de facto standard that enterprises can use to implement Identity Federation.

Term	Description
SAML Assertion	A core element in the SAML protocol to describe the authentication request and response. For example, specific properties of a user are contained in the authentication response assertion.
Trust	A Mutual Trust mechanism between an SP and an IdP. It is usually implemented by using public and private keys. An SP obtains the Identity Federation metadata of an IdP through a circle of trust establishment. The metadata includes the public key for verifying the SAML Assertion issued by the IdP. The SP can use the public key to verify the assertion integrity.

SAML federated SSO process

In the scenario where Alibaba Cloud services are integrated with an enterprise identity system, Alibaba Cloud is the SP, and the enterprise identity system is the IdP. The following figure shows the ways enterprise employees can log on to the Alibaba Cloud console through their enterprise identity services.



As shown in the figure, after the administrator configures the services provided by an enterprise IdP, the enterprise's employees can log on to the Alibaba Cloud console by performing the following steps:

1. An enterprise employee logs on to Alibaba Cloud through a browser, and Alibaba Cloud returns an SAML authentication request to the browser.
2. The browser forwards the request to the enterprise IdP.
3. The enterprise IdP prompts the RAM user to log on and returns an SAML response to the browser.
4. The browser forwards the SAML response to Alibaba Cloud.
5. With the SAML Mutual Trust configuration, Alibaba Cloud verifies the digital signature of the SAML response and the authenticity of the SAML Assertion, and then matches the RAM user's identity according to the user name configured in SAML Assertion.
6. After the logon service is verified, Alibaba Cloud returns the logon session and the URL of the Alibaba Cloud console to the browser.
7. The browser redirects to the Alibaba Cloud console.

> Note:
> In step 1, the employee is not required to log on to Alibaba Cloud. Instead, the employee can click the link on the enterprise IdP portal to send an SAML authentication request to the enterprise IdP and access the console.

SAML federated SSO configuration

Before configuring SAML federated SSO, you must establish the mutual trust between your Alibaba Cloud account and your enterprise IdP.

For example, your enterprise is using some IdPs that are compatible with SAML 2.0, such as AD FS, Google G Suite, and Shibboleth. The following describes how to perform the general configuration:

1. Configure the Alibaba Cloud account as a trusted SAML SP in an external IdP.
   a. Obtain the SAML Service Provider Metadata URL of your account from Alibaba Cloud. For details, see *Configure the SAML of an external IdP*.
   b. On the IdP side, use the metadata to register your account as a SP and establish the mutual trust between your enterprise IdP and Alibaba Cloud account.
   c. Customize an SAML assertion in the external IdP.

      The IdP and SP must achieve common understanding of the SAML assertion to better understand the description of a user identity. Alibaba Cloud uses a User Principal Name (UPN) to locate a RAM user. Therefore, the SAML response generated by an external IdP must contain the UPN of the RAM user. Alibaba Cloud resolves the NameID node in the SAML assertion and matches the UPN of the RAM user, so that the federated SSO can be implemented.

      That means, when you customize the SAML assertion issued by an IdP, you need to map the UPN of a RAM user to the NameID in the SAML assertion.
2. Configure a trusted external SAML IdP in the Alibaba Cloud account.

   To establish the mutual trust between Alibaba Cloud and your enterprise IdP, you must configure your IdP to Alibaba Cloud using the SAML metadata provided by the enterprise IdP. The metadata includes the IdP service address, the public key for verifying the SAML assertion, and the assertion format. Common IdP services provide the specific URLs for downloading the SAML metadata. For details, see *Configure the SAML of an account*.
3. Provision users.

   After establishing the mutual trust between the SP and the IdP, you must create one or more RAM users that correspond to users in the enterprise IdP. Only RAM users can use SSO authentication. You cannot use SSO for your account.

   You can provision the users using either of the following methods:

   - Log on to the RAM console and manually create the RAM users that match the enterprise IdP.
   - Use a RAM SDK to write a program or use aliyuncli to customize a solution.

After the preceding configurations are complete, the federated SSO can be implemented between RAM users and an enterprise IdP. When a RAM user in a account logs on to Alibaba Cloud, Alibaba Cloud automatically directs to the URL of

your enterprise IdP for the user to log on. After the logon succeeds, the Alibaba Cloud console is automatically displayed.

2.3.2 Configure the SAML of an external IdP

When configuring Alibaba Cloud SAML federated Single Sign On (SSO), you must configure the SAML of an external IdP, set an Alibaba Cloud account as an SP through SAML, and establish trust between the external IdP and the Alibaba Cloud account. This topic describes how to configure the SAML of an external IdP.

Configure an Alibaba Cloud account as a trusted SAML SP

1. Obtain the SAML Service Provider Metadata URL of your account from Alibaba Cloud.
   a. Log on to the *RAM console*.
   b. Choose Identities > Settings > Advanced. Then, in the Setup SSO area, obtain the SAML Service Provider Metadata URL.
2. Create an SAML SP in an external IdP and configure the SAML Service Provider Metadata URL of Alibaba Cloud.

   Note:
   If your IdP does not support URL configuration, click the URL next to SAML Service Provider Metadata URL to download an XML file. Then, when you create an SAML SP, you can upload the XML file.

Customize an SAML assertion in an external IdP

Alibaba Cloud uses a User Principal Name (UPN) to locate a RAM user. Therefore, the SAML response generated by an external IdP must contain the UPN of the RAM user. Alibaba Cloud resolves the NameID node in the SAML assertion and matches the UPN of the RAM user, so that the federated SSO can be implemented.

That means, when you customize the SAML assertion issued by an IdP, you must map the UPN of a RAM user to the NameID in the SAML assertion.

Example

The processes of configuring an SAML SP and customizing an SAML assertion vary according to the IdP system. This topic provides an example of how to implement SSO from Microsoft Active Directory (AD) to Alibaba Cloud, detailing the end-to-end

configuration process from an enterprise IdP to Alibaba Cloud Identity Federation. For details, see *Example*.

2.3.3 Configure the SAML of an account

This topic describes how to configure the SAML of an Alibaba Cloud (the SP) account, including how to set the default domain name, domain alias, and Single Sign On (SSO).

Set the default domain name of an account

Each account has a Default domain. To view and modify it, you can log on to the *RAM console* and choose Identities > Settings > Advanced.

- The format of the Default Domain is <$AccountAlias>.onaliyun.com.
- If you have not set an account alias, the default account alias is AccountID. The format of the Default Domain is <$AccountID>.onaliyun.com.

Set a domain alias for the default domain name

A Domain Alias simplifies the SAML SSO configuration.

On the Domain Management page, you can create a Domain Alias for the Default Domain. We recommend that you set the Domain Alias to the real domain name of your enterprise for easier management.

For example, if your default domain name is secloud.onaliyun.com and the domain alias is secloud.net, a RAM user can use alice@secloud.onaliyun.com or alice@secloud.net for logon.

Create a domain alias

1. Log on to the RAM console and choose Identities > Settings > Advanced.
2. Click Create Domain Alias.
3. Enter the domain name.
4. Click OK.
5. Click Domain Ownership Validation.

Note:
After you successfully create a domain alias, you need to copy the verification code and set the DNS TXT record on the domain purchase platform. You can click Domain Ownership Validation then do this.

Set SAML SSO

1. Log on to the RAM console and choose Identities > Settings > Advanced. The status of Setup SSO is displayed.
2. Click SSO Settings.
   - Metadata File: A metadata file, usually in XML format, is provided by an external IdP. It contains the IdP's logon service address and X.509 public key certificate that is used to verify the validity of the SAML assertion issued by the IdP.
   - SSO Status: You can set it to Enabled or Disabled.
     - The default value is Disabled. When the SSO function is disabled, the RAM users can use their passwords for logon, and all SSO settings do not take effect.
     - If you select Enabled, the RAM users cannot use their passwords for logon. They must log on to the external IdP service for identity authentication. If the SSO function is disabled later, the page for logon using passwords will be automatically displayed.

 Note:
The SSO function only takes effect for the RAM users under an account. It does not affect the primary account directly.

2.3.4 Provision users

This topic describes how to provision users and how to use the RAM user synchronization tool to quickly synchronize the RAM users from Microsoft Active Directory (AD) or an LDAP directory to RAM.

You can migrate or synchronize user data from an enterprise IdP to Alibaba Cloud RAM using one of the following methods:

- Log on to the RAM console and manually create the RAM users that match the enterprise IdP.
- Use a RAM SDK to write a program or use aliyuncli to customize a solution.
- Use the Alibaba Cloud RAM user synchronization tool to synchronize users from the enterprise IdP to Alibaba Cloud RAM.

 Note:

To use the RAM user synchronization tool for a trial, contact your account manager.

Install and configure the RAM user synchronization tool

- The synchronization tool must run on a Microsoft Windows server.
- After installing the tool, perform the following steps:

1. Configure the local IdP service address.
2. Configure a user account and a password for the synchronization tool to read IdP directory data.

   Notice:
   You must grant the user the permission to read AD.
3. Configure an AccessKey for the synchronization tool to call Alibaba Cloud RAM APIs.

   Notice:
   We recommend that you use the AccessKey of a RAM user that has obtained relevant RAM API permissions.

2.3.5 Example

This topic provides an example of how to implement Single Sign On (SSO) from Microsoft Active Directory (AD) to Alibaba Cloud, detailing the end-to-end configuration process from an enterprise identity provider (IdP) to Alibaba Cloud Identity Federation.

Implement SSO from Microsoft AD to Alibaba Cloud

This topic uses Windows Server 2012 R2 as an example to describe how to configure Microsoft AD as the SSO IdP of Alibaba Cloud.

Notice:
Note that the configuration of Microsoft AD described in this example is for reference only.

Prerequisites

Microsoft AD has been properly configured and the following server roles have been configured on Windows Server 2012 R2:

- DNS server: resolves and sends identity authentication requests to the correct Federation Service.
- Active Directory Domain Service (AD DS): creates, queries, and modifies objects such as domain users and domain devices.
- Active Directory Federation Service (AD FS): configures the Identity Federation relying party and performs SSO authentication for the configured relying party.

Example configuration

The configuration in the example is as follows:

- Default domain name of the account: `secloud.onaliyun.com`.
- RAM user under the account: `alice`. The User Principal Name (UPN) is `alice@secloud.onaliyun.com`.
- AD FS of the self-built Microsoft AD: `adfs.secloud.club`.
- Domain name of the self-built Microsoft AD: `secloud.club`. The NETBIOS is `secloud`.
- UPN of the user (alice) in Microsoft AD: `alice@secloud.club`. The user can also use `secloud\alice` for intra-domain logon.

Configure AD FS as a trusted SAML IdP in RAM

1. Enter the following URL in your browser:

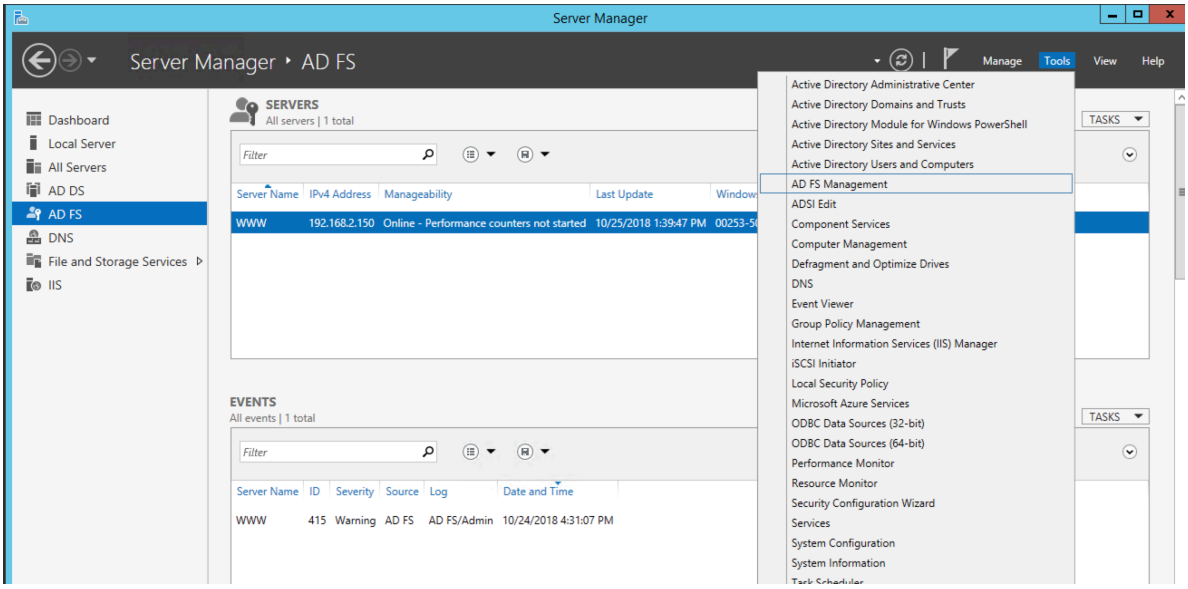
```
https://adfs.secloud.club/FederationMetadata/2007-06/Federation
Metadata.xml
```

2. Download the metadata file in XML format.
3. In the RAM console, use the metadata file for SSO configuration.

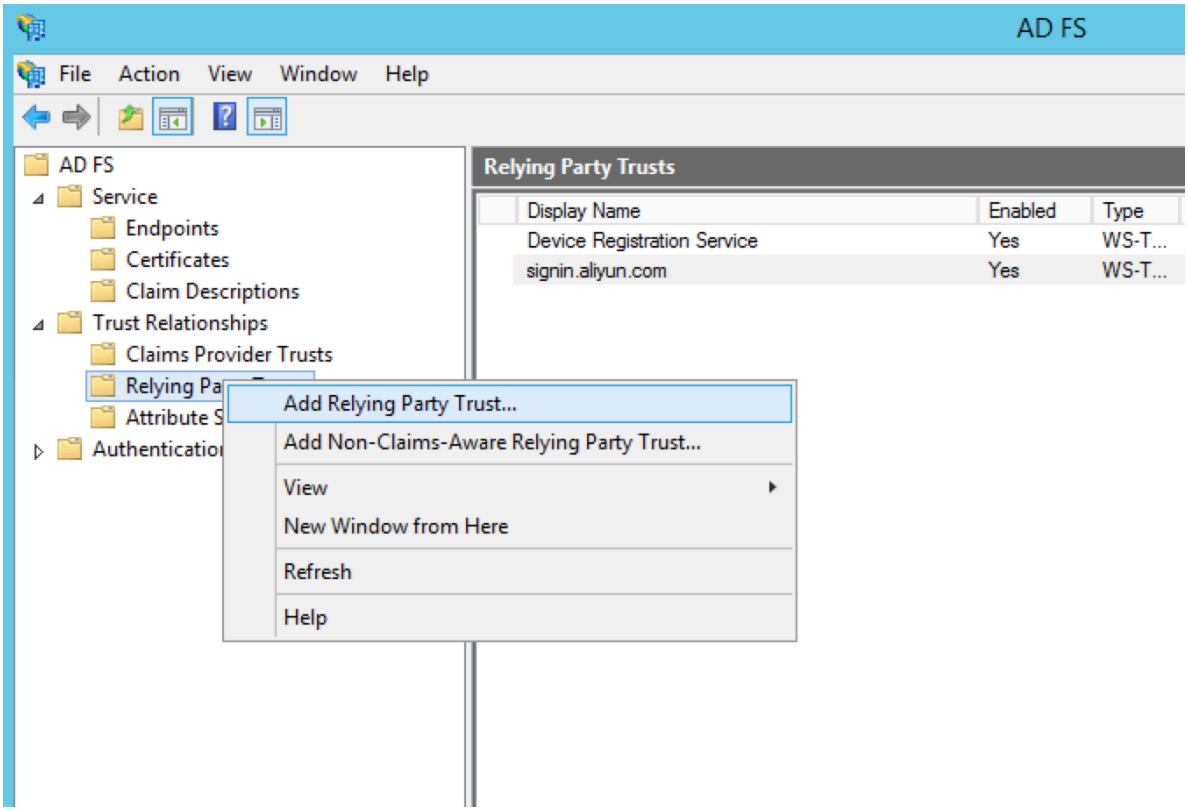
Configure Alibaba Cloud as a trusted SAML SP in AD FS

In AD FS, SAML SP is called Relying Party. To configure Alibaba Cloud as a trusted SP, perform the following steps:

1. On the Server Manager page, click Toolsand selectAD FS Management.

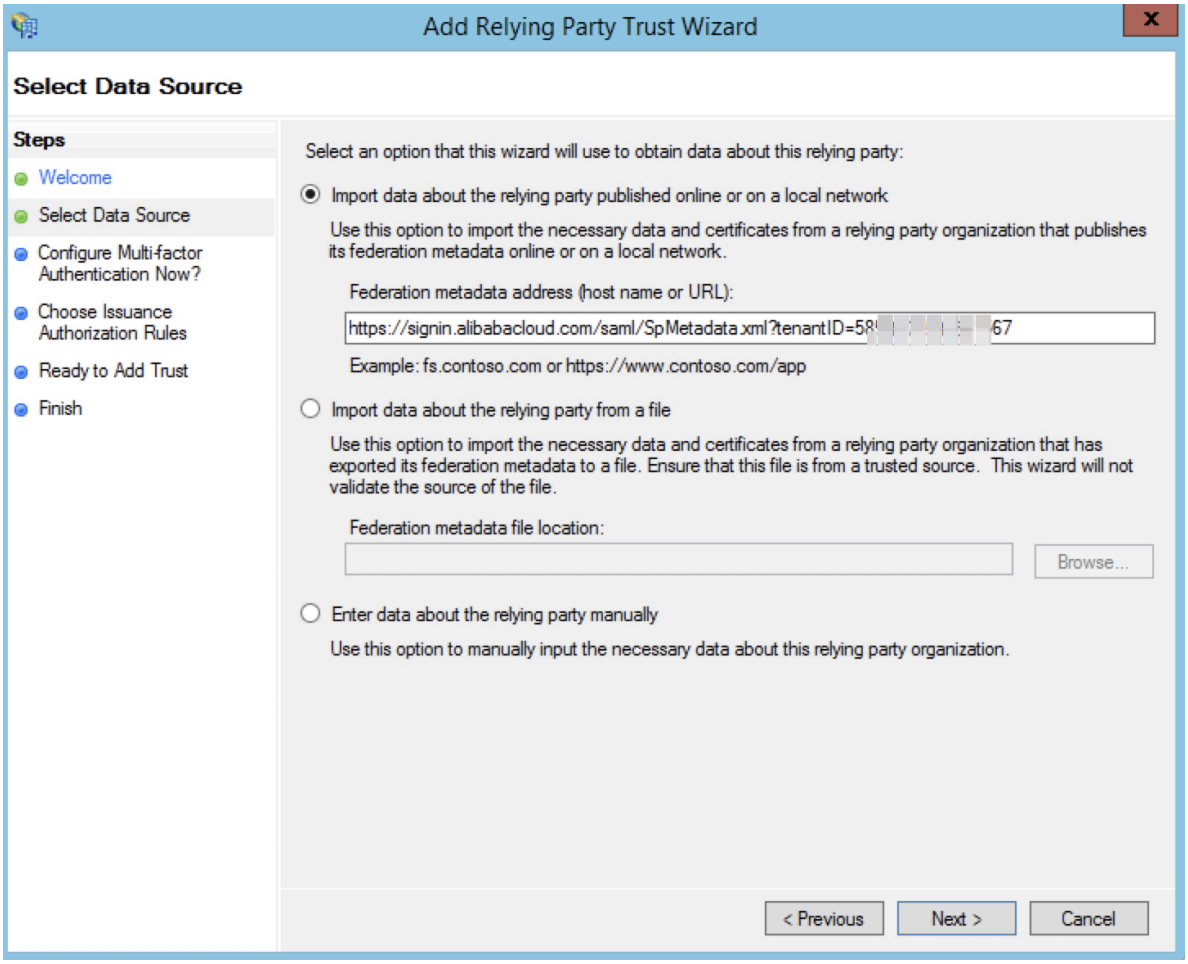


2. Select Add Relying Party Trust.



3. Set the SAML metadata of Alibaba Cloud for the relying party.

   To view the SAML metadata URL, log on to the RAM console and choose Identities > Settings > Advanced. You can enter the metadata URL when configuring the AD FS relying party.



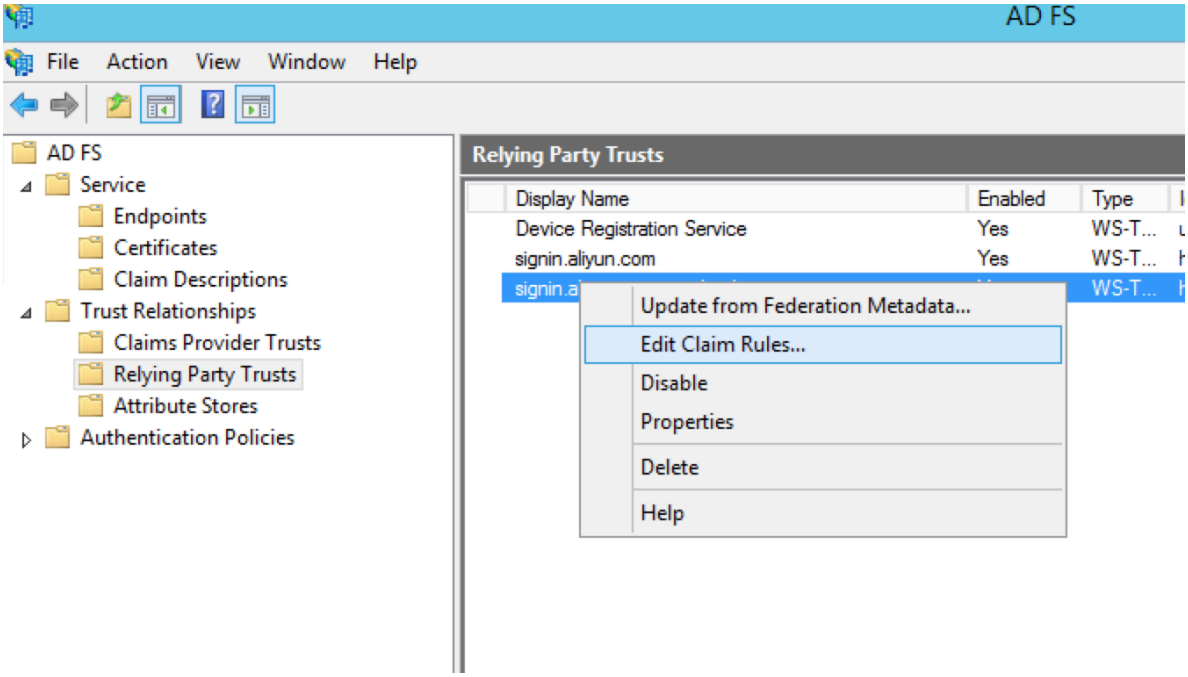
   After the relying party is configured, Alibaba Cloud sends an authentication request of the RAM user whose domain name is `secloud.onaliyun.com` to AD FS `adfs.secloud.club` . AD FS also receives the request from Alibaba Cloud and sends an authentication response to Alibaba Cloud.

Configure the SAML assertion attributes for the Alibaba Cloud SP

We recommend that you set the value of the NameID field in the SAML assertion to the UPN of the RAM user, so that Alibaba Cloud can locate the correct RAM user according to the SAML response.

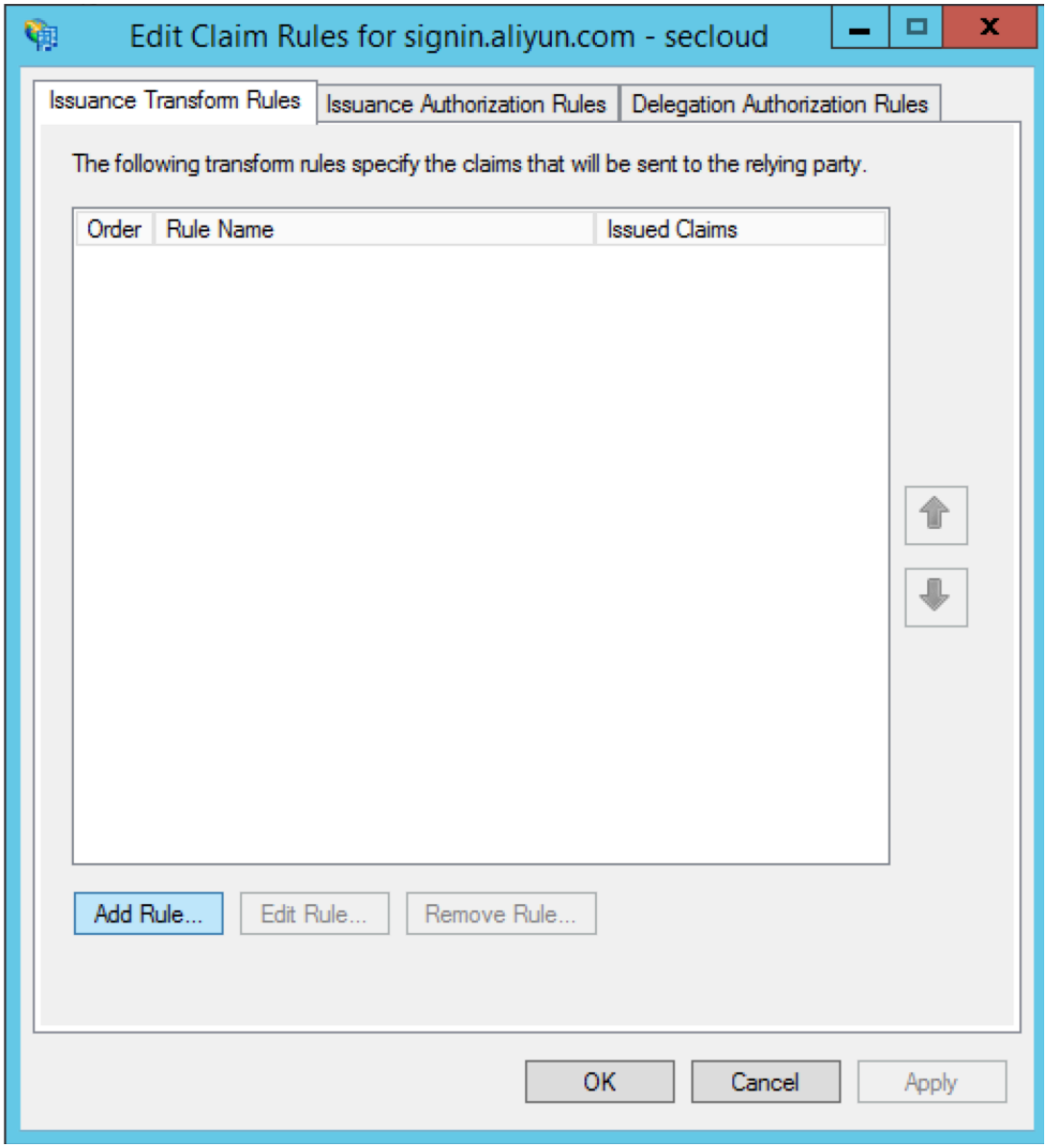
You must set the UPN in the AD to the NameID in the SAML assertion. The procedure is as follows:

1. Select Edit Claim Rules.

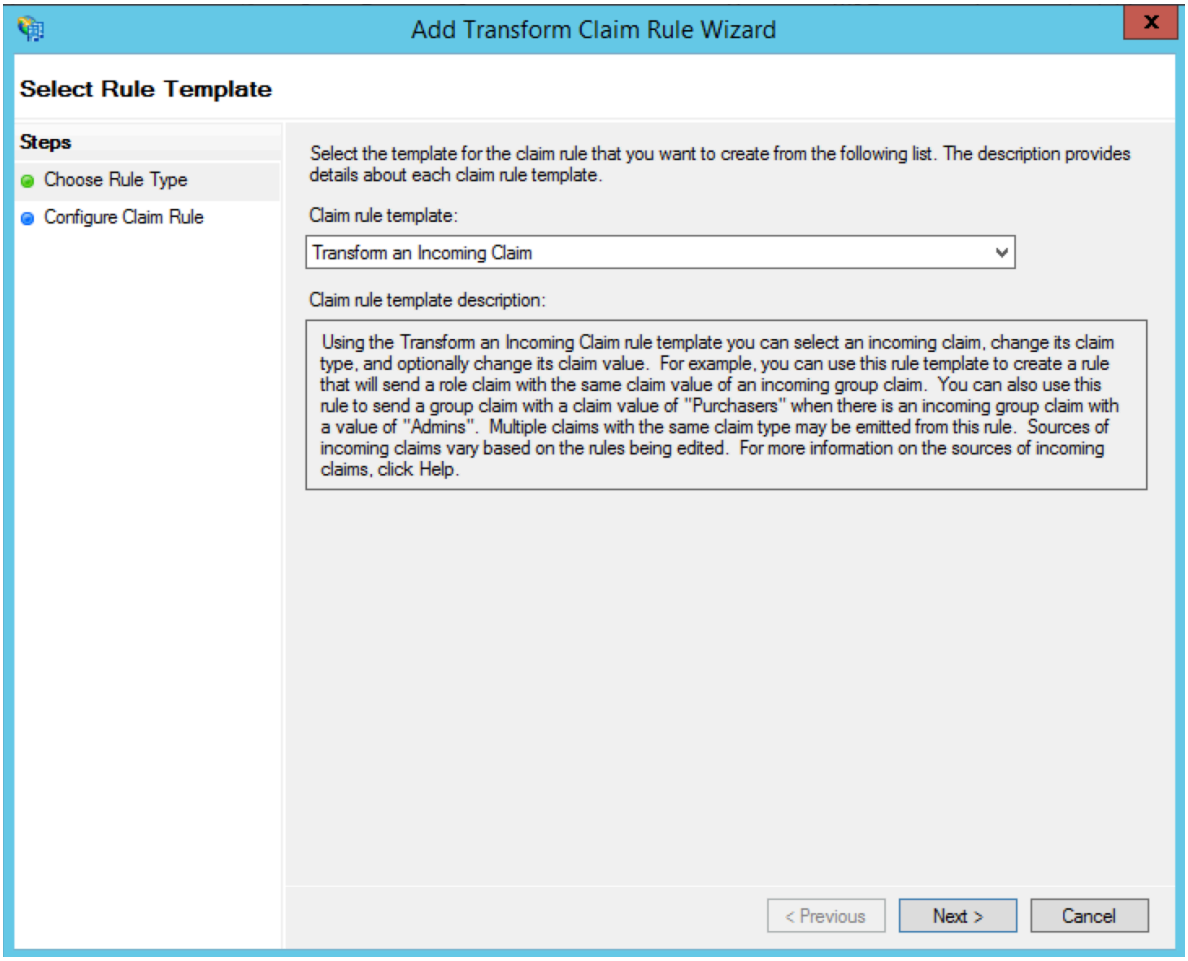


2. Click Issuance Transform Rules to add a rule.

   Issuance Transform Rules: indicates how to transform a known user attribute and issue it as an attribute in the SAML assertion. You must issue the UPN of a user in Microsoft AD as a NameID. This means that a new rule is required.



3. Set Claim rule template to Transform an Incoming Claim.



4. Select Edit Rule.

   In this example, the domain name of the UPN in the account is `secloud.onaliyun.com`, and the domain name of the UPN in Microsoft AD is `secloud.club`. If you directly map the UPN in Microsoft AD to the NameID, Alibaba Cloud cannot match the correct user.

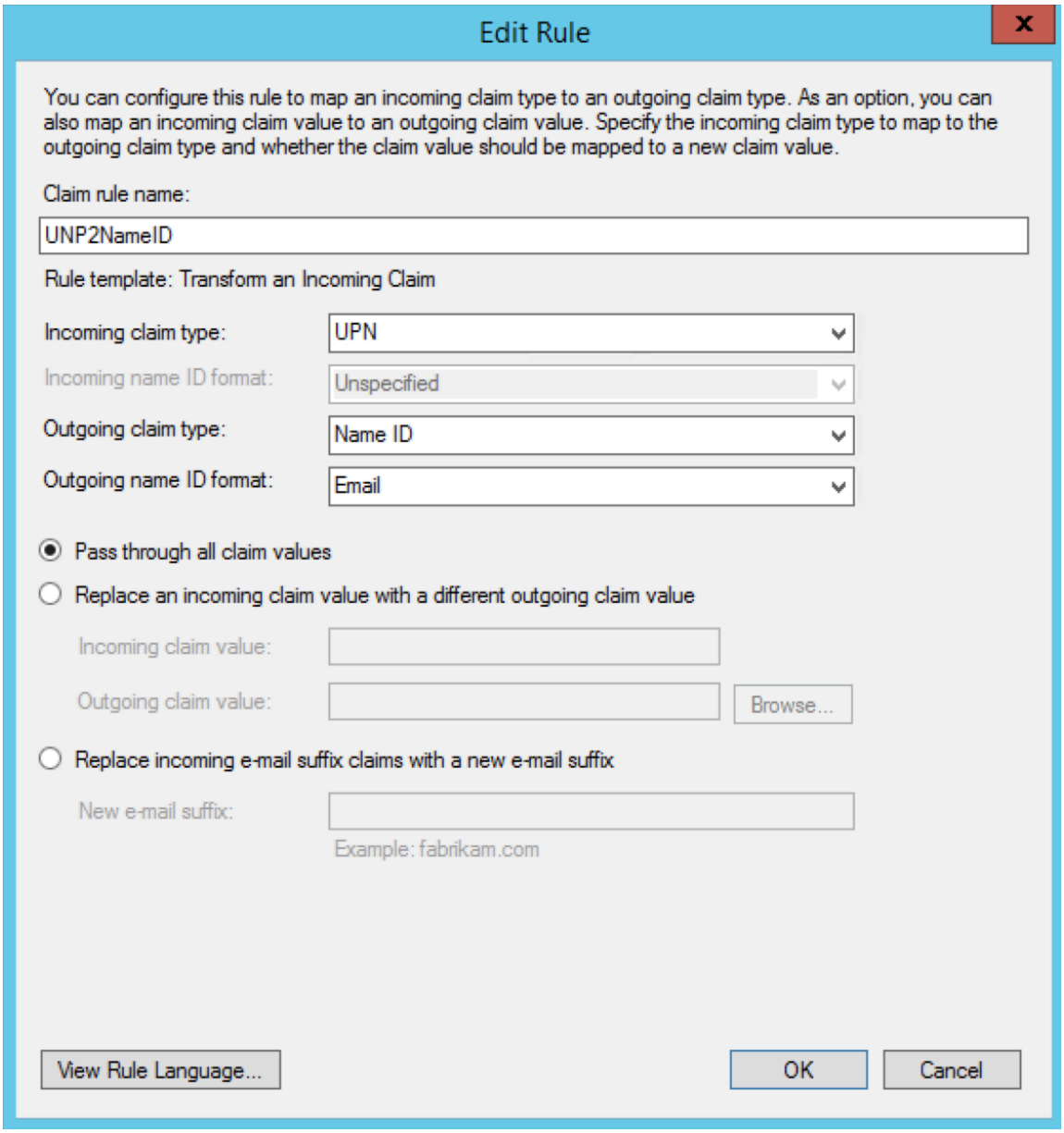
   To solve this problem, use either of the following methods:

   a. Method 1: Set the domain name of Microsoft AD to the domain alias of RAM.

      If the domain name `secloud.club` of Microsoft AD is registered in a DNS on the Internet, you can set `secloud.club` to the domain alias of RAM. For details, see

Configure the SAML of an account. After the setting is successful, the UPN of the RAM user is the same as that of the Microsoft AD user.

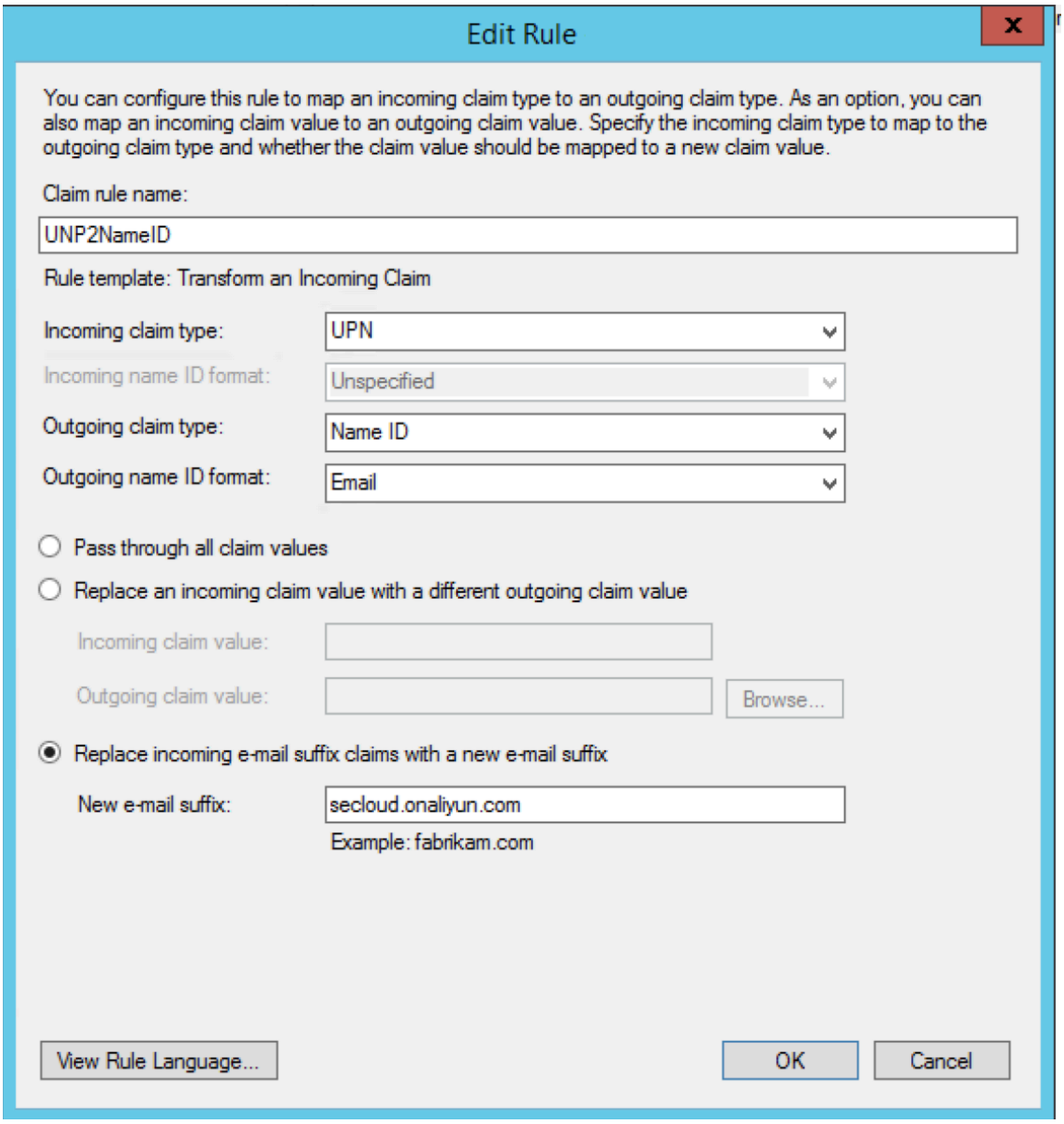
In the Edit Rule window, map the UPN to the NameID.



b. Method 2: Transform the domain names in AD FS.

If the domain name `secloud.club` is an intranet domain name of an enterprise, Alibaba Cloud cannot verify the domain ownership of the enterprise. RAM can only use the default domain name `secloud.onaliyun.com`. In this case, in the

SAML assertion issued by AD FS to Alibaba Cloud, you must replace the domain name suffix `secloud.club` of the UPN with `secloud.onaliyun.com`.



2.4 RAM roles and identities

2.4.1 Understand RAM roles

RAM roles, similar to RAM users, are a type of identity defined in RAM. Compared with RAM users, RAM roles are virtual users, and do not have specific identity authentication keys. RAM roles can be used only when the roles are assumed by trusted entity users.

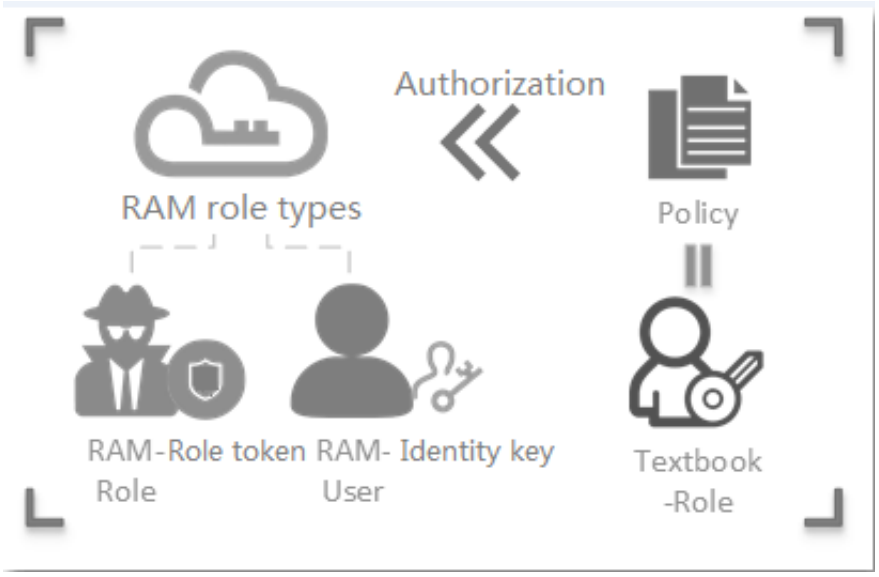
Note:

In this topic, roles refer to RAM roles unless otherwise specified.

Understand RAM roles

RAM roles (RAM-Role) are also known as virtual users. They are a type of RAM identity.

Figure 2-1: RAM roles



- RAM roles are different from textbook roles (Textbook-Role). A textbook role (or a traditionally defined role) indicates a permission set, similar to a policy in RAM. If such a role is granted to a user, the user has a set of permissions and can access the authorized resources.
- As virtual users, RAM roles have specific identities and can be granted a set of policies. However, RAM roles do not have specific identity authentication keys (logon passwords or AccessKeys).

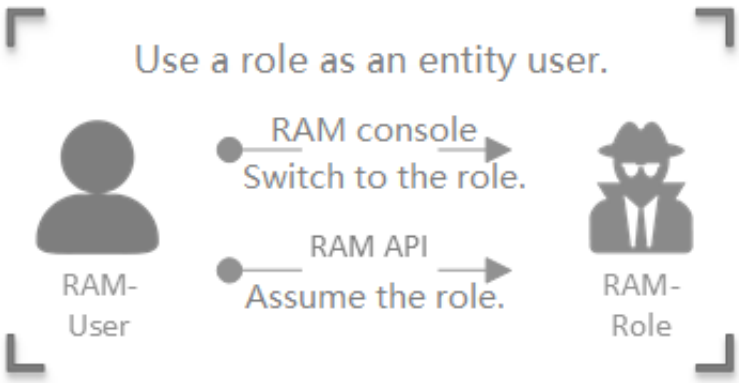
  Entity users and virtual users differ in whether a user can be directly authenticated or not.

  - Entity users have specific logon passwords or AccessKeys (AKs). Accounts, RAM user accounts, and cloud service accounts are examples of entity users.
  - Virtual users do not have specific authentication keys. RAM roles are an example of entity users.
- Compared with RAM users, RAM roles can be used only after they are assumed by trusted entity users. The entity users obtain temporary security tokens of the RAM roles, and then use the tokens to access the authorized resources as role identities.

Instructions

RAM roles are valid only when they are attached to a trusted entity.

Figure 2-2: Use RAM roles



- If an entity user wants to use an authorized RAM role, the entity user must log on as its own identity, and then switch its identity from the entity identity to role identity.

  Note:
  Then, the entity user can perform operations authorized for this role identity, and its own access permission is temporarily unavailable.

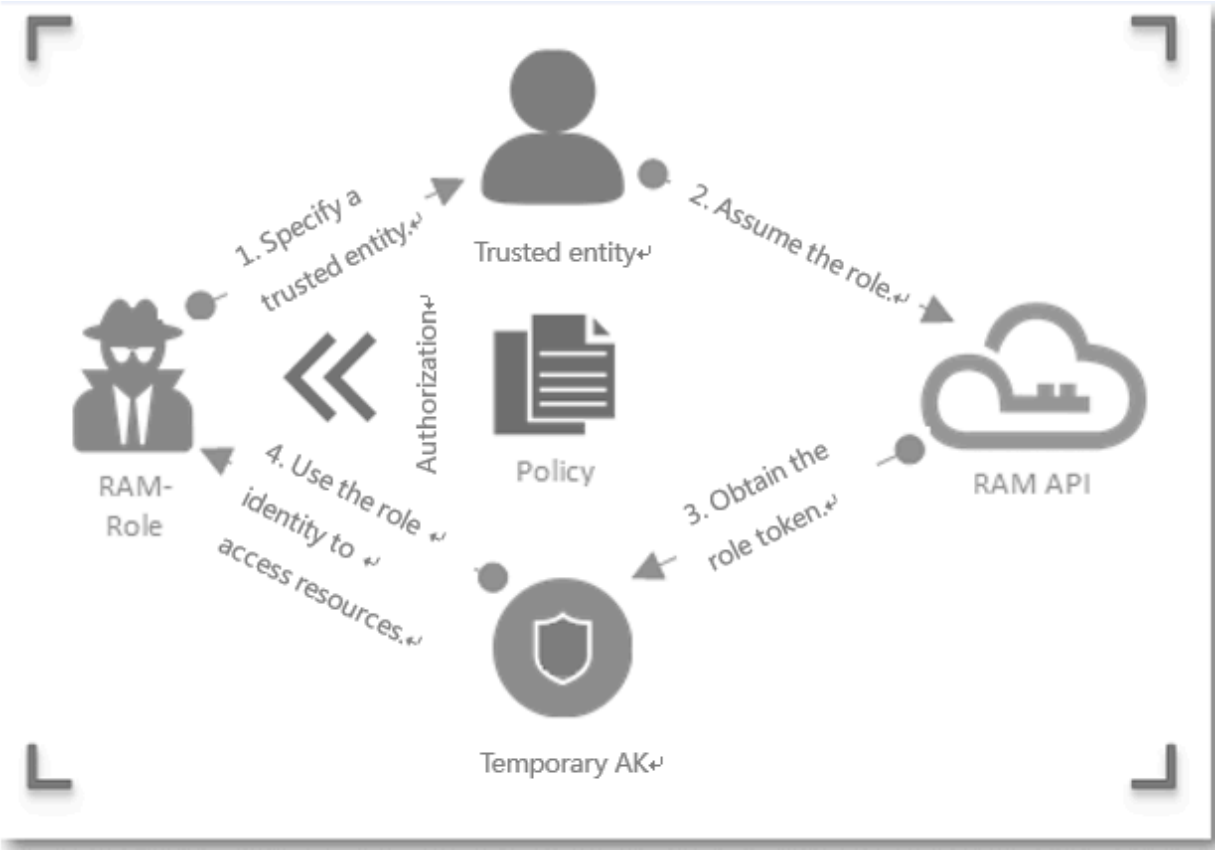
- If the entity user wants to switch from the role identity back to entity identity, the user only needs to switch to the logon identity.

  Note:
  Then, the entity user's own access permission becomes valid, and the user no longer retains the permission owned by the role identity.

Related concepts

The following figure illustrates the relationships between the concepts related to RAM roles.

Figure 2-3: Concepts related to RAM roles



The following table describes these concepts:

Concept	Description
RoleARN	A RoleARN is the global resource identifier of a role. It is used to specify a role. · RoleARNs conform to Alibaba Cloud ARN naming conventions. For example, the ARN of the role devops under an account is `acs:ram::1234567890123456:role/samplerole`. · After creating a role, you can click the role name and find its ARN in the Basic Information area.

Concept	Description
Trusted entity	A trusted entity is the identity of a trusted entity user who can assume a role. · You must specify a trusted entity when creating a role. Only trusted entities can assume roles. · A trusted entity can be a trusted account or service.
Policy	A role can be attached to a set of policies . Roles that are not attached to any policy can exist, but cannot be used.
Role assuming	Role assuming (Assume Role) is the method for entity users to obtain security tokens of roles. By calling the AssumeRole API, an entity user can obtain the security token of a role and use the token to access cloud service APIs .
Identity switching	Identity switching (Switch Role) is the method for entity users to switch from the logon identity to role identity in the RAM console. · After logging on to the RAM console, an entity user can switch to a role that the user can assume. The user can then use the role identity to operate cloud resources. After switching to the role identity, the user's own access permission will be temporarily unavailable. · When the user no longer needs the role identify, the user can switch back to its logon identity.
Role token	A role token is a temporary access key to a role identity. RAM roles do not have specific identity authentication keys. When an entity user wants to use a role, the user must assumes the role to obtain the role token. Then, the user can use the role token to call Alibaba Cloud service APIs.

RAM role types

RAM roles are divided into the following types according to different trusted players:

- Alibaba Cloud Account: roles that RAM users can assume. The RAM users may belong to their own accounts or other accounts. Such roles provide solutions to cross-account access and temporary authorization.
- Alibaba Cloud Service: roles that cloud services can assume. Such roles are used to authorize cloud services to operate resources on your behalf.

Scenarios

- *Temporary authorization for mobile apps*
- *Cross-account resource authorization and access*
- *Dynamic identity and permission management of cloud applications*

2.4.2 Manage RAM roles

This topic describes how to manage RAM roles.

> **Note:**
> In this topic, roles refer to RAM roles unless otherwise specified.

Create a RAM role

1. Create an Alibaba Cloud Account.
   a. Log on to the *RAM Console*.
   b. Choose RAM Roles > Create RAM Role.
   c. In the displayed dialog box, select Alibaba Cloud Account for Select type of trusted entity.
   d. Select an account type.
      - If you create a role for RAM users under your account (for example, authorizing mobile app clients to directly operate OSS resources), select Current Alibaba Cloud Account as the trusted account.
      - If you create a role for RAM users under another account (for example, cross-account resource authorization), select Other Alibaba Cloud Account and enter the account ID.
   e. Enter RAM Role Name. You can also choose to enter Note. Then, click OK.

2. Create an Alibaba Cloud Service.

   a. Log on to the *RAM Console*.

   b. Choose RAM Roles > Create RAM Role.

   c. In the displayed dialog box, select Alibaba Cloud Service for Select type of trusted entity.

   d. Select Trusted Service as needed. Available service roles include:

      - Media Transcoding Service (MTS): You can create such a role, configure MTS as its trusted service, and use MTS to assume the role and access OSS data when you set OSS Bucket as the data source for MTS tasks.
      - Archive Storage Service (OAS): You can create such a role, configure OAS as its trusted service, and use OAS to assume the role and access OSS data when you set OSS Bucket as the data source for OAS.
      - Log Service (LOG): You can create such a role, configure LOG as its trusted service, and use LOG to assume the role and write data into OSS when you import LOG-collected logs into OSS.
      - API Gateway (ApiGateway): You can create such a role, configure API Gateway as its trusted service, and use API Gateway to assume the role and call the function service when you set the function service as the backend service of API Gateway.
      - Elastic Compute Service (ECS): You can use such a role to authorize ECS to access your cloud resources in other cloud services.

       Note:
      For more trusted services, see the RAM console.

   e. Enter RAM Role Name. You can also choose to enter Note. Then, click OK.

   The created role has no permission. You can click Add Permissions to directly grant permissions to the role. For the authorization method, see *Permission granting in RAM*.

   Return to the RAM Console home page. In the RAM Roles pane, locate the created role and click RAM Name to view the role details.

Use a RAM role

Alibaba Cloud Service can be assumed only by trusted cloud services, while Alibaba Cloud Account can be assumed by RAM users.

1. Create a RAM user and create an AccessKey (AK) or set a password for the user.
2. Add the system policy AliyunSTSAssumeRoleAccess to authorize the RAM user.

 Note:
For maintain account security, trusted accounts are not allowed to assume roles by their own identities. Roles must be assumed by RAM users.

RAM users can assume roles either in the RAM console or through APIs:

- Assume RAM roles in the RAM console
  1. Log on to the RAM Console as a RAM user.
  2. In the upper-right corner, hover your mouse over your account icon and click Switch Role.
  3. In the displayed Switch Role dialog box, enter the account alias and role name, and then click Switch.

     The RAM user logs on to the RAM console as the role identity. In this case, both the current role identity and the user's logon identity are displayed in the upper-right corner.
  4. Click Switched Login Role to switch back to the user's logon identity.
- Assume RAM roles through APIs

  After being granted the AssumeRole permission, a RAM user can use its AK to call the AssumeRole API of Security Token Service (STS) to obtain the temporary security token of a role. Then, the user uses the token to access cloud resource APIs. For details about how to call the AssumeRole API, see *AssumeRole*.

3 Permission management

3.1 Policy overview

Alibaba Cloud uses permissions to describe the authorized actions of RAM identities (such as RAM users, user groups, and roles) to access specific resources. Permissions determine whether an operation can be performed on some resources under certain conditions. A policy is a set of access permissions.

Permission

- An account (resource owner) controls all permissions.
  - Each resource has only one owner. The owner must be an account and has full resource control permissions.
  - The resource owner is not necessarily the resource creator. For example, if a RAM user has permission to create resources, the resources created by this RAM user belong to the RAM user's account. The RAM user is the resource creator, but is not the resource owner.
- By default, a RAM user has no permissions.
  - A RAM user is an operator and must be granted explicit permission before performing any operations.
  - A new RAM user has no operation permissions by default, and cannot perform operations on resources through the console or APIs until being granted permission.
- A resource creator (RAM user) is not automatically granted permissions for the created resources.
  - A RAM user can create resources if the user is granted the resource creation permission.
  - However, the RAM user is not automatically granted any permissions for the created resources, unless the resource owner explicitly grants permission to the user.

Policy

A policy is a set of permissions described in *Policy language syntax*. It can accurately describe the authorized resource sets, operation sets, and authorization conditions a user can be granted with. With a policy being attached, a user or user group can obtain the specified access permissions in the policy. If the policy has both Allow and Deny statements, Deny takes priority.

In RAM, a policy is a resource entity that can be created, updated, deleted, and viewed by users. RAM supports the following two types of policies:

- System policy: A system policy is a group of common permissions provided by Alibaba Cloud. The permissions include read-only permissions or full permissions for different products that are commonly used. System policies cannot be modified by users. The policies are automatically upgraded by Alibaba Cloud.
- Custom policy: If no system policy meets your requirements, you can create a custom policy as needed. For example, if you want to control the operation permissions for a certain ECS instance or want the resource operation requests to come from specified IP addresses, you must use a custom policy.

Grant permission to RAM identities

Granting permission to RAM identities is to attach one or more policies to the RAM users, user groups, or roles.

- The attached policy can be either a system policy or a custom policy.
- If the attached policy is updated, the updates to the policy automatically take effect , and you do not need to attach the policy again.

3.2 Policy management

Types of policies include system policies and custom policies. System policies can be viewed but cannot be modified. Custom policies can be created to meet your needs as required.

Create a custom policy

Before you create a custom policy, we recommend that you read about the basic structure and syntax of a policy. For details, see *Policy language syntax*.

1. Log on to the *RAM console*.
2. Choose Permissions > Policies.

3. Click Create Policy.
4. Enter the Policy Name and Note.
5. Set Configuration Mode to Visualized or Script.
   - If you set it to Visualized, click Add Statement and configure the permission effect, actions, and resources as prompted.
   - If you set it to Script, edit the policy according to *Policy language syntax*.

Modify a custom policy

If the permissions of a user are changed (added or removed), you must modify the user's policy. You may have the following requirements when modifying a policy:

- You still want to use the old policy after a period of time.
- You want to restore a previous policy version if the current version has incorrect modifications.

To address these issues, a version management function is provided.

- You can retain multiple versions for a policy.
- If you reach the maximum number of policy versions allowed, we recommend that you delete versions you no longer need to save space.
- Even if a policy has multiple versions, only one version is active. The active version is known as the default version.

1. In the RAM console, choose Permissions > Policies.
2. In the Policy Name column, click the policy to be managed.

    Note:
   You can enter keywords to search for a specific policy.
3. Click Versions, then you can:
   - Click View to view the policy content of all historical versions.
   - Click Use This Version to set the target version policy to the default version.
   - Click Delete to delete a target version.

Delete a custom policy

You can create multiple policies and maintain multiple versions for each policy. For custom policies that are no longer needed, we recommend that you delete them.

Prerequisites

Before deleting a policy, ensure that:

- The policy has only one version, the default version. If multiple versions exist, you must delete all of the versions except the default one.
- The policy is not referenced (that is, attached to a user, user group, or role). If the policy is currently being referenced, click Revoke Permission on the References page.

Procedure

1. In the RAM console, click Permissions.
2. In the Policy Name column, find the policy to be deleted and click Delete.

   
   Note:
   You can enter keywords to search for a specific policy.
3. In the Delete Custom Policy dialog box, click OK.

   
   Note:
   The policy cannot be deleted if it has been referenced.

3.3 Permission granting

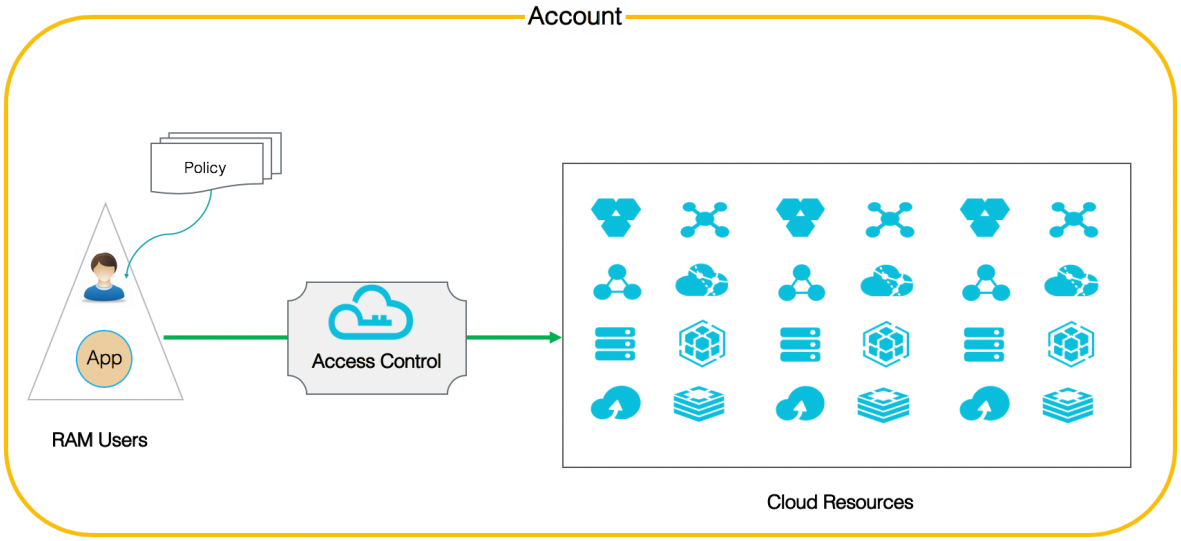
3.3.1 Permission model overview

Alibaba Cloud allows you to grant permissions for an account or for a resource group. You can select an appropriate model according to your specific requirements.

Grant permissions for an account

Granting permissions for an account means that when you attach a policy to a RAM identity, all resources under the account are included within the scope of the policy permissions.

Figure 3-1: Model of granting permissions for an account



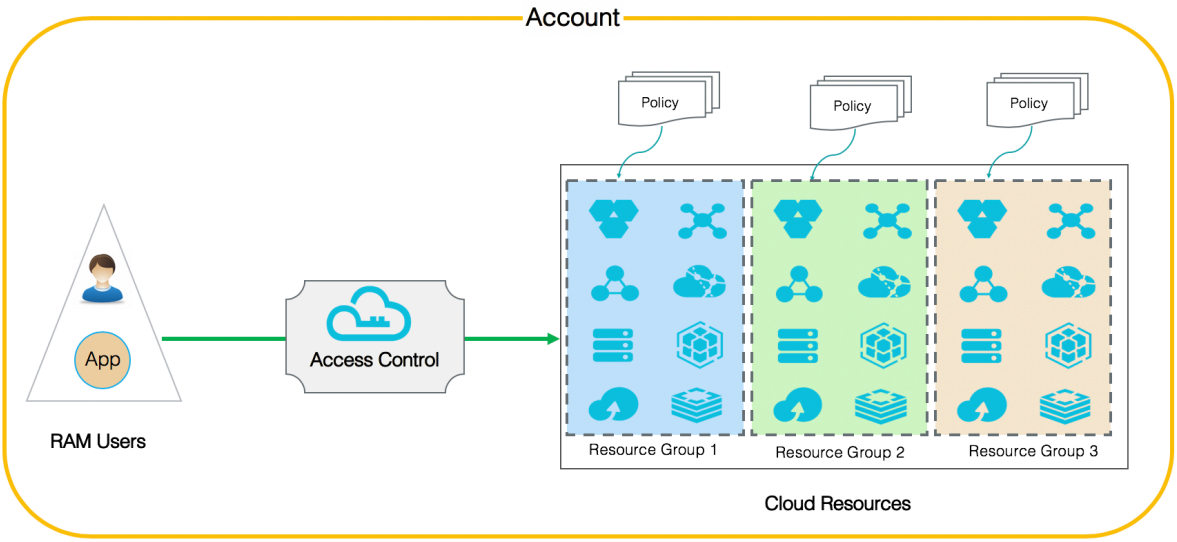
Grant permissions for one or more target resource groups

Granting permissions for a resource group means that when you attach a policy to a RAM identity, only the resources within the target resource group are included within the scope of the policy permissions.

In detail, the user with the `AdministratorAccess` system policy in a resource group is called administrator. By default, the resource group creator is assigned as

administrator. The administrator is the entity that can add RAM users to the resource group and grant permission to the users in the resource group.

Figure 3-2: Model of granting permissions for a resource group



3.3.2 Permission granting in RAM

This topic describes how to grant permission to RAM identities in an account. For details about granting permission to RAM identities in a resource group, see the documents related to resource management.

Granting permission in RAM refers to attaching one or more policies to a RAM identity (a RAM user, user group, or role).

- Granting permission to RAM users or user groups mainly refers to granting permission to your organization members.
- Granting permission to RAM roles mainly refers to granting permission in complex cloud application scenarios, for example, temporary authorization for mobile device applications, cross-account resource authorization, dynamic identity and authorization management for cloud applications, and authorization for operations between cloud services.

Grant permission to a RAM user or a user group

When granting permission to the RAM users under your current account, you can grant permission to a specific user or the group to which the user belongs. If you grant permission to a user group, all users in the group share the same permissions.

Grant permission to a RAM user

1. Log on to the *RAM console*.
2. Choose Identities > Users.
3. In the User Logon Name/Display Name column, find the user to be granted and click Grant Permission.
   - In the Policy Name column on the left, select the policies to be attached to the user. The policies are added to the area on the right.

      Note:
     You can enter keywords to search for a specific policy.
   - To remove a policy, select the policy from the area on the right, and then click X.
4. Click Ok.

Grant permission to a user group

1. Log on to the *RAM console*.
2. Choose Identities > Groups.
3. In the Group Name/Display Name column, find the user group to be granted and click Add Permissions.
   - In the Policy Name column on the left, select the policies to be attached to the user group. The policies are added to the area on the right.

      Note:
     You can enter keywords to search for a specific policy.
   - To remove a policy, select the policy from the area on the right, and then click X.
4. Click Ok.

Grant permission to a RAM role

When you create a RAM role, you can select the trusted entity as Alibaba Cloud Account (the current Alibaba Cloud account or other Alibaba Cloud accounts) or Alibaba Cloud Service. You need to enter the corresponding trusted account ID or select the trusted service (that is, allow the service to use the created role to access your cloud resources).

- If you select Alibaba Cloud Account and Current Alibaba Cloud Account, the RAM users under the current account can assume the RAM role and therefore authorized to access the required cloud resources.
- If you select Alibaba Cloud Account and Other Alibaba Cloud Account, the RAM users under other specified accounts can assume the RAM role and therefore authorized to access the required cloud resources.
- If you select Alibaba Cloud Service, the trusted cloud services can assume the RAM role and therefore authorized to access the required cloud resources.

1. Log on to the *RAM console*.
2. Click RAM Roles.
3. In the Role Name column, find the role to be granted and click Add Permissions.
   - In the Policy Name column on the left, select the policies to be attached to the role. The policies are added to the area on the right.

     Note:
     You can enter keywords to search for a policy.
   - To remove a policy, select the policy from the area on the right, and then click X.
4. Click Ok.

3.4 Policy language

3.4.1 Elements

RAM uses policies to describe the details of a permission. Generally, a policy includes the following elements: Effect, Resource, Action, and Condition.

Effect

Effect can be either Allow or Deny.

Resource

Resources are the objects being authorized.

For example, in the policy "User A is allowed to perform the GetBucket operation on the resource SampleBucket", the resource is SampleBucket.

Action

Actions are operations performed on specific resources.

For example, in the policy “User A is allowed to perform the GetBucket operation on the resource SampleBucket”, the action is GetBucket.

Condition

Conditions are the circumstances under which a permission takes effect.

For example, in the policy "User A is allowed to perform the GetBucket operation on the resource SampleBucket before 2011-12-31", the condition is "before 2011-12-31".

Example

In the following policy example, read-only permissions for the OSS resource SampleBucket are allowed on condition that the source IP address of the requester is 42.160.1.0.

```
{
      "Version": "1",
      "Statement":
        [{
          "Effect": "Allow",
            "Action": ["oss:List*", "oss:Get*"],
            "Resource": ["acs:oss:*:*:samplebucket", "acs:oss:*:*:
samplebucket/*"],
            "Condition":
             {
                "IpAddress":
                 {
                    "acs:SourceIp": "42.160.1.0"
                  }
              }
         }]
```

```
}
```

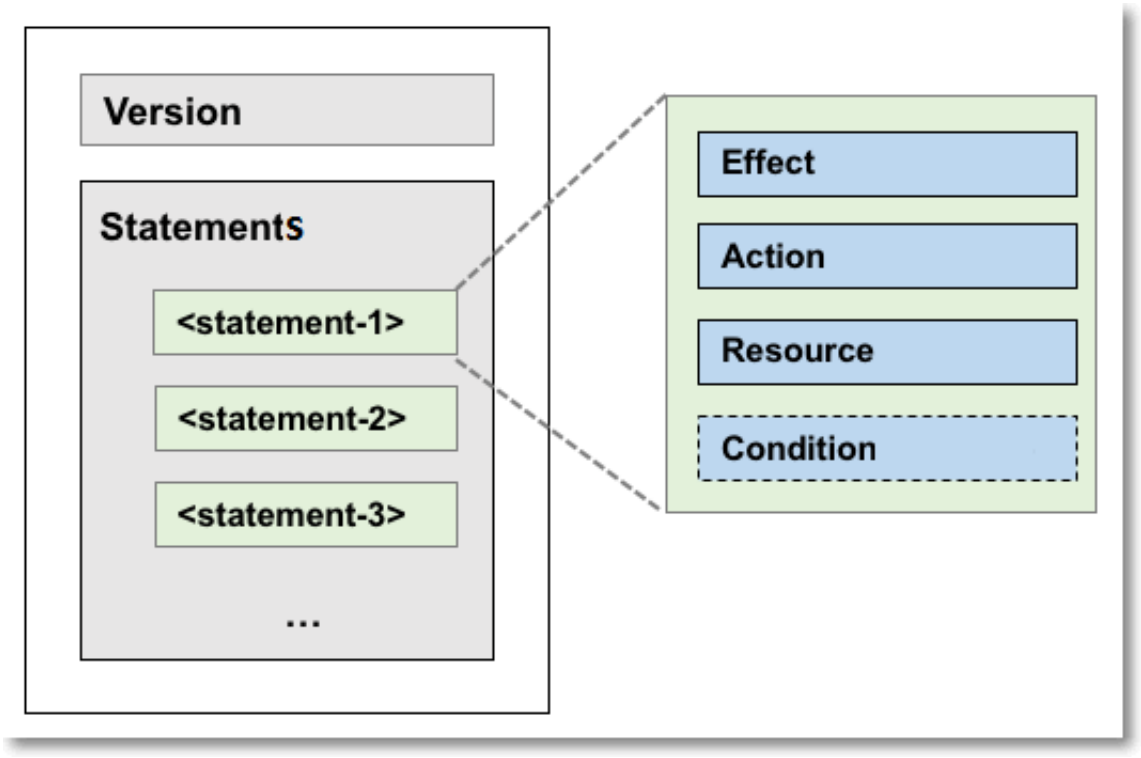
3.4.2 Policy language syntax

This topic describes the policy language syntax and policy rules in RAM.

Policy language syntax

The policy language syntax includes the version number and a list of statements. Each statement contains the following elements: Effect, Action, Resource, and Condition. The Condition element is optional.

Figure 3-3: Policy language syntax



Format check (JSON)

RAM policies must be expressed in JSON. When you create or update a policy, RAM first checks whether the JSON format is correct.

- For details about the JSON syntax standards, see *RFC 7159*.
- We recommend that you use tools such as JSON validators and editors to verify your policies to meet JSON syntax standards.

Policy syntax

The characters, rules, and syntaxes of a policy are described as follows:

Characters and rules

The JSON characters in a policy include `{ } [ ] " , :`. The special characters used to describe the policy syntaxes include `= < > ( ) |`.

The syntax character conventions are as follows:

- If an element can have multiple values, each value is indicated by a comma (,) as the delimiter, and ellipses (...) in the syntax to describe the rest of the values. For example, `[ <action_string>, <action_string>, ...]`. Elements that support multiple values also support single values. This means that the two descriptions `"Action": [<action_string>]` and `"Action": <action_string>` are equivalent.
- An element with a question mark (?) in the syntax indicates that it is an optional element, for example, `<condition_block? >.`
- If multiple values are separated by vertical bars (|) in the syntax, only one of the values can be selected, for example, `("Allow" | "Deny")`.
- An element enclosed with double quotation marks ("") is a text string, for example, `<version_block> = "Version" : ("1")`.

Policy syntax and description

A policy syntax is as follows:

```
policy  = {
     <version_block>,
     <statement_block>
}
<version_block> = "Version" : ("1")
<statement_block> = "Statement" : [ <statement>, <statement>, ... ]
<statement> = {
    <effect_block>,
    <action_block>,
    <resource_block>,
    <condition_block? >
}
<effect_block> = "Effect" : ("Allow" | "Deny")
<action_block> = ("Action" | "NotAction") :
    ("*" | [<action_string>, <action_string>, ...])
<resource_block> = ("Resource" | "NotResource") :
    ("*" | [<resource_string>, <resource_string>, ...])
<condition_block> = "Condition" : <condition_map>
<condition_map> = {
  <condition_type_string> : {
      <condition_key_string> : <condition_value_list>,
      <condition_key_string> : <condition_value_list>,
      ...
  },
  <condition_type_string> : {
      <condition_key_string> : <condition_value_list>,
      <condition_key_string> : <condition_value_list>,
      ...
```

```
  }, ...
}
<condition_value_list> = [<condition_value>, <condition_value>, ...]
<condition_value> = ("String" | "Number" | "Boolean")
```

Description:

- Version: The current policy version is 1.
- Statement: A policy can have multiple statements.
  - Each statement can be either Deny or Allow. In a statement, Action is a list of operations, and Resource is a list of objects.
  - Each statement supports its own conditions. A condition block can contain multiple conditions with different operation types and logical combinations of these conditions.
- Deny takes priority: You can grant multiple polices to a user. If these polices contain both Allow and Deny statements, Deny takes priority (that is, the Deny statements overwrite the Allow statements).
- Element value:
  - If an element value is a number or Boolean, it must be enclosed using double quotation marks ("") like strings.
  - If an element value is a string, characters such as the asterisk (*) and question mark (?) can be used for fuzzy matching.
    - The asterisk (*) indicates any number (including zero) of allowed characters.

      
      Note:
      For example, `ecs:Describe*` indicates all ECS actions starting with Describe.
    - The question mark (?) indicates one allowed character.

Rules for using the policy elements

The rules for using the elements in a policy are described as follows:

Effect

The Effect value is either Allow or Deny, for example, `"Effect": "Allow"`.

Action (operation list)

Action can have multiple values. The values are API operations defined by the target cloud services. The format is defined as follows:

```
<service-name>:<action-name>
```

 Note:
In general, a RAM action corresponds to a product API. For other cases, see the corresponding product documents.

Format description:

- service-name: name of an Alibaba Cloud product, such as ecs, rds, slb, oss, and ots.
- action-name: service-related API operations.

Example:

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

Resource (resource list)

Resource generally specifies the object of operations, such as the ECS virtual machine instances and OSS storage buckets. In a policy, the resources of Alibaba Cloud services are formatted as follows:

```
acs:<service-name>:<region>:<account-id>:<relative-id>
```

Format description:

- `acs`: abbreviation of Alibaba Cloud Service, indicating the Alibaba Cloud public cloud platform.
- `service-name`: name of a service provided by Alibaba Cloud, such as ecs, oss, and ots.
- `region`: region information. If this option is not supported by the service, use an asterisk (*).
- `account-id`: account ID, such as `1234567890123456`. It can be replaced with an asterisk (*).
- `relative-id`: service-related resource description. Its meaning is specified by a specific service. relative-id is similar to a file path. For example, `relative-id = “mybucket/dir1/object1.jpg”` indicates an OSS object.

Description example:

```
"Resource": ["acs:ecs:*:*:instance/inst-001", "acs:ecs:*:*:instance/
inst-002", "acs:oss:*:*:mybucket", "acs:oss:*:*:mybucket/*"]
```

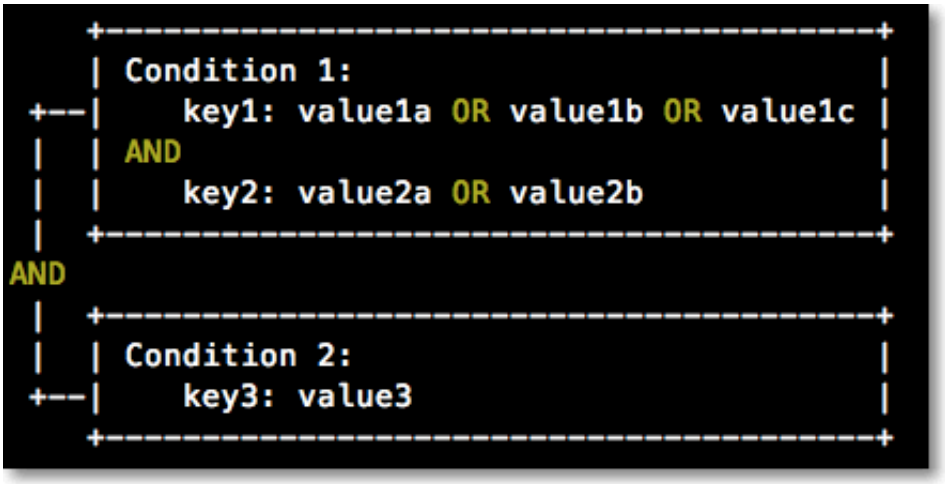
Condition

A condition block consists of one or more condition clauses. A condition clause consists of an operation type, a keyword, and a condition value. The operation type and keyword will be described later in this topic.

Condition block judgment logic

The following figure describes the logic for determining whether a condition is satisfied.

Figure 3-4: Logic for determining whether a condition is satisfied



The details are as follows:

- For each condition keyword, one or more condition values can be specified. When conditions are evaluated, if the runtime value of the condition keyword matches any of the corresponding values, the condition is satisfied.
- A condition clause is satisfied only if multiple conditions of the same condition operation type are all satisfied.
- A condition block is satisfied only if all of its condition clauses are satisfied.

Condition operation type

The following types of condition operations are supported: String, Numeric, Date and time, Boolean, and IP address.

Operations in each condition operation type are listed as follows.

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

Condition keyword (condition-key)

The condition keywords reserved by Alibaba Cloud services use the following naming format:

```
acs:<condition-key>
```

The common condition keywords reserved by Alibaba Cloud services are as follows.

Common condition keyword	Type	Description
`acs:CurrentTime`	Date and time	Time when the Web server receives a request. This keyword is described in ISO 8601 format, for example, `2012-11-11T23:59:59Z`.
`acs:SecureTransport`	Boolean	Indicates whether a secure channel, such as HTTPS, is used to send a request.
`acs:SourceIp`	IP address	IP address of the client that sends a request.
`acs:MFAPresent`	Boolean	Indicates whether Multi-Factor Authentication is used during user logon.

Some cloud services define product condition keywords. These keywords are in the following format:

```
<service-name>:<condition-key>
```

The condition keywords defined by some cloud services are as follows.

Service	Condition keyword	Type	Description
ECS	`ecs:tag/<tag-key>`	String	Tag keyword for ECS resources. This keyword can be customized by users.
RDS	`rds:ResourceTag/<tag-key>`	String	Tag keyword for RDS resources. This keyword can be customized by users.
OSS	`oss:Delimiter`	String	Separator used by OSS to group the object names.
OSS	`oss:Prefix`	String	Prefix of an OSS object name

Policy example

The following policy example contains two statements:

- The first statement grants the permission to view all ECS resources (`ecs:Describe*`) in China East 1 (Hangzhou) Region.
- The second statement grants two read-only permissions (`oss:ListObjects`, `oss:GetObject`) for objects in the OSS bucket mybucket, and allows only users with the source IP address of `42.120.88.10` or `42.120.66.0/24`.

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecs:Describe*",
            "Resource": "acs:ecs:cn-hangzhou:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
```

```
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:mybucket",
                "acs:oss:*:*:mybucket/*"
            ],
            "Condition":{
                "IpAddress": {
                    "acs:SourceIp": ["42.120.88.10", "42.120.66.0/24"]
                }
            }
        }
    ]
}
```

3.4.3 Policy example

This topic describes how to create a policy and details the basic elements, policy structure, and policy syntax involved.

The following is a policy example, which contains two statements:

- **The first statement grants the permission (`ecs:Describe*`) to view all ECS resources in China East 1 (Hangzhou) Region.**
- **The second statement grants two read-only permissions (`oss:ListObjects` and `oss:GetObject`) to access objects in the OSS bucket mybucket, and allows access to resources only from users with the source IP address of `42.120.88.10` or `42.120.66.0/24`.**

```
{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecs:Describe*",
            "Resource": "acs:ecs:cn-hangzhou:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "oss:ListObjects",
                "oss:GetObject"
            ],
            "Resource": [
                "acs:oss:*:*:mybucket",
                "acs:oss:*:*:mybucket/*"
            ],
            "Condition":{
                "IpAddress": {
                    "acs:SourceIp": ["42.120.88.10", "42.120.66.0/24"]
                }
            }
        }
    ]
```

```
}
```

3.5 Permission check rules

This topic describes the permission check model and rules to help you better understand the RAM policies.

Basic model

You can access resources in RAM using an account, or as an authorized RAM user or RAM role. RAM determines whether to allow access according to the rules described in the following table.

Access type	Rules
Account	The account is the resource owner. Note: Some cloud services, such as Log Service, support cross-account ACL authorization. If the ACL authorization is successful, access is allowed even the account is not the resource owner.
RAM user	· The account to which the RAM user belongs has permission to access the resources. · The account has attached a policy with explicit Allow effect to the RAM user.
RAM role	· The account to which the RAM role belongs has permission to access the resources. · The account has attached a policy with explicit Allow effect to the RAM role. · If a policy is attached when the RAM role's STS token is generated, the policy must have an explicit Allow effect.

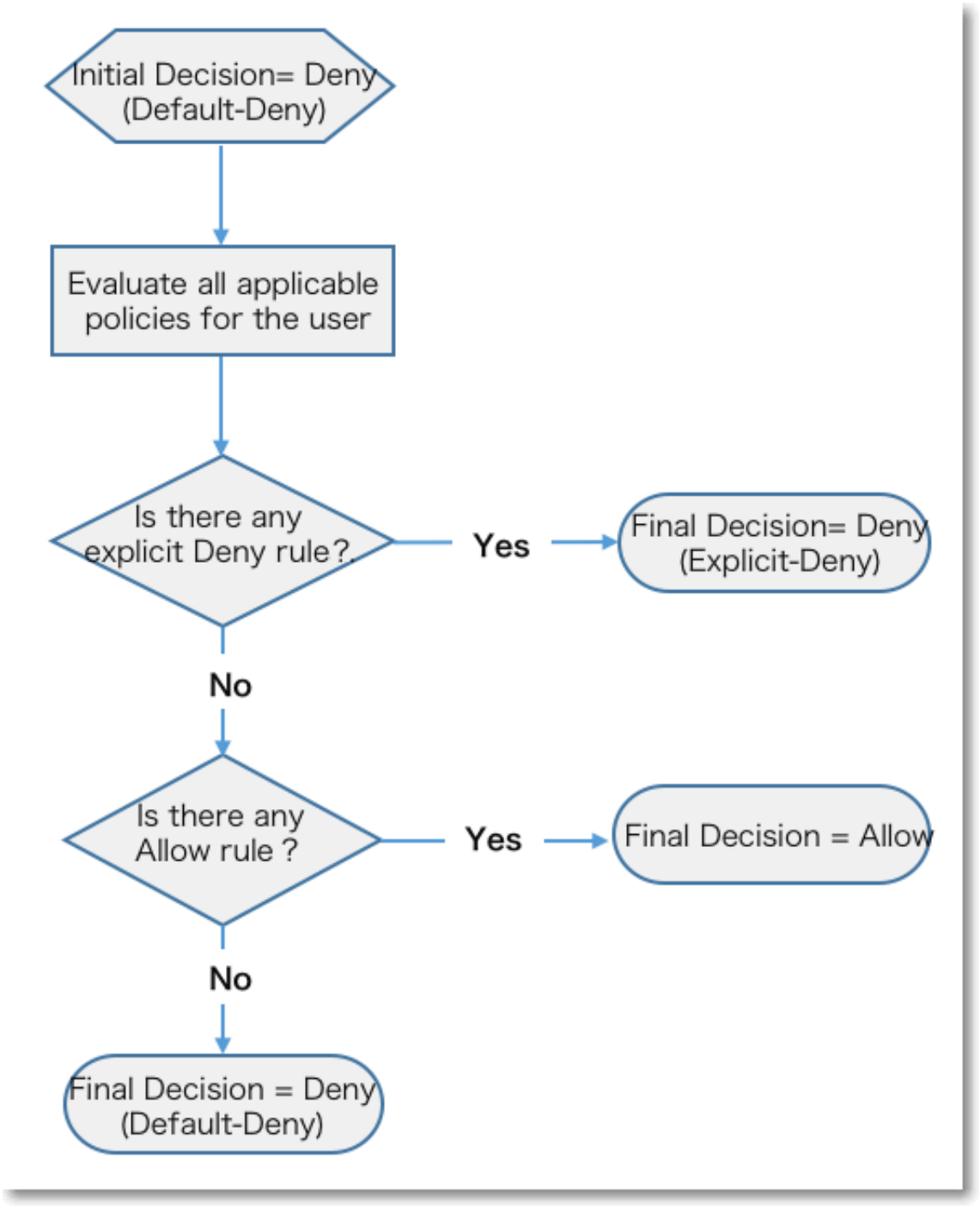
Permission check logic for RAM users

By default, RAM users do not have resource access permissions unless they have been granted explicit permission by the account (that is, a policy has been attached to

them). A policy supports Allow and Deny statements. When multiple statements grant Allow and Deny permissions for the same resource operation, Deny takes priority.

The following figure shows the policy check logic.

Figure 3-5: Policy check logic



When you access the resources as a RAM user, the permission check logic is as follows:

1. The system checks the policy attached to the RAM user.
   - If the result is Deny, access is denied.
   - Otherwise, go to the next step.
2. The system checks whether the account of the RAM user has the resource access permission.
   - If the account is the resource owner, access is allowed.
   - If the account is not the resource owner, the system checks whether the account has the cross-account ACL permission on the resource.
     - If yes, access is allowed.
     - If no, access is denied.

Permission check logic for RAM roles

When you access resources as a RAM role (that is, using an STS token), the permission check logic is as follows:

1. If the STS token has a specified policy (that is, it uses the policy parameters set when AssumeRole is called), the policy check logic described in the preceding section is implemented.
   - If the result is Deny, access is denied.
   - Otherwise, go to the next step.

   If the STS token does not have a specified policy, the system automatically goes to the next step.
2. The system checks the policy attached to the RAM role.
   - If the result is Deny, access is denied.
   - Otherwise, go to the next step.
3. The system checks whether the account of the RAM role has the resource access permission.
   - If the account is the resource owner, access is allowed.
   - If the account is not the resource owner, the system checks whether the account has the cross-account ACL permission on the resource.
     - If yes, access is allowed.
     - If no, access is denied.

4 Scenarios

4.1 User management and access control

Scenario description

Assume that EnterpriseA has bought several types of cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets, for Project-X. In this project, multiple employees need to perform operations on these cloud resources. For example, some employees are responsible for procurement, some for operation and management, and some for online application. Different employees require different permissions to complete different operations. In detail:

- For security reasons, EnterpriseA does not want to disclose the AccessKey (AK) of its Alibaba Cloud account to its employees. Instead, it wants to create different RAM users for its employees and grant different permissions to these RAM users.
- The employees can then perform resource operations as RAM users only after the users are granted the relevant permissions, and the fees incurred by these operations are not billed to the RAM users but to the corresponding Alibaba Cloud account.
- EnterpriseA can revoke the permissions granted to the RAM users and delete the RAM users at any time.

Requirement analysis

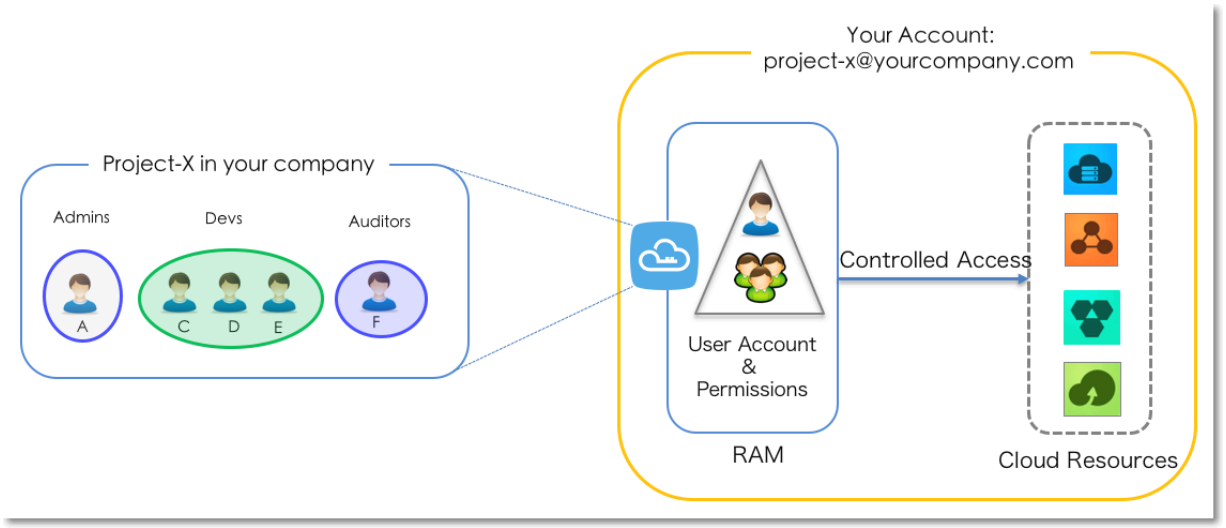
The requirements of the preceding scenario are analyzed as follows:

- Employees do not share the Alibaba Cloud account to avoid mistaken disclosure of the account password or AK.
- Independent RAM users are created for different employees and the RAM users are granted independent permissions.
- All operations of all users can be audited.
- Fees are not charged to each RAM user, but are instead charged to the correspond ing Alibaba Cloud account to which the RAM users belong.

Solution

Use the permission management function, as shown in the following figure:

Figure 4-1: Permission management



The procedure is as follows:

1. *(Optional) Set MFA* to avoid risks associated with mistaken exposure of the Alibaba Cloud account password.
2. Activate RAM service.
3. *Create a RAM user*. Create RAM users for different employees (or applications) and set logon passwords or create AKs.
4. *(Optional) Create a RAM user group*. If multiple RAM users require the same permissions, we recommend that you create a user group and add the corresponding users to this user group.
5. *Permission granting in RAM*. Attach one or more system policies to the groups or users. For finer-grained permission management, you can create one or more custom policies and attach them to individual users or to a user group. For more information, see *Create a custom policy*.

4.2 Temporary authorization for mobile apps

This topic describes how to use the RAM role STS token to grant temporary permissions to mobile apps.

Scenario description

EnterpriseA has developed a mobile app and wants to use Alibaba Cloud OSS so that the mobile app can upload data to and download data from OSS. Because the mobile app runs on user devices, these devices cannot be directly managed by EnterpriseA. The restrictions that EnterpriseA has are as follows:

- EnterpriseA does not want the app to use the appServer to transmit data. Instead, it wants the app to directly upload data to and download data from OSS.
- To maintain account security, EnterpriseA will not save the AccessKey (AK) in the app.
- EnterpriseA wants to minimize its security risks by granting the app temporary access credentials (by means of a security token) that the app can then use to connect to OSS, thereby restricting the access duration to a specified period of time (for example, 30 minutes).

Requirement analysis

The requirements of the preceding scenario are analyzed as follows:

- The mobile app needs to directly transmit data from and to OSS, without using a data proxy.
- The AK cannot be stored to the mobile app because mobile devices are not managed by EnterpriseA directly. The best practice is to use an access token with expiration time.
- The access permission of the mobile app must be restricted, to the OSS object level.

Solution

Use the RAM role STS token to authorize temporary access to OSS.

- Use EnterpriseA's cloud account (Account A) to create a role in RAM, grant appropriate permissions to the role, and allow the appServer (logs on as a RAM user) to use this role.

  For details, see *Create a role, create a user, and grant permissions*.

- When an app needs to connect directly to OSS to upload or download data, the appServer can assume a role (call STS AssumeRole API) to get a temporary security token (STS token) and transfer it to the app. Then, the app can use the temporary security token to access the OSS API directly.

  For details, see *Get and pass the role token*.

- The appServer can further limit the resource operation permissions of the temporary security token when it assumes the role, to control the permissions of each app at a finer-grained authorization level.

  For details, see *Restrict STS token permissions*.

Create a role, create a user, and grant permissions

Assume that the account ID of Account A is 11223344. The process to create a role, create a user, and grant permissions for the appServer is as follows:

1. Account A creates a user role (here, the role is named oss-readonly) and selects Current Alibaba Cloud Account as the trusted account so that only RAM users under Account A can assume this role. For details, see *Manage RAM roles*.

   After creating the role, EnterpriseA can get the role information on the role details page.

   - In this example, the role's Alibaba Cloud Resource Name (ARN) is:

     ```
     acs:ram::11223344:role/oss-readonly
     ```

   - The role’s trust policy is as follows:

     ```
     {
     "Statement": [
     {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::11223344:root"//when the role is a user role, it is
      permanently set to root
        ]
      }
     }
     ],
     "Version": "1"
     }
     ```

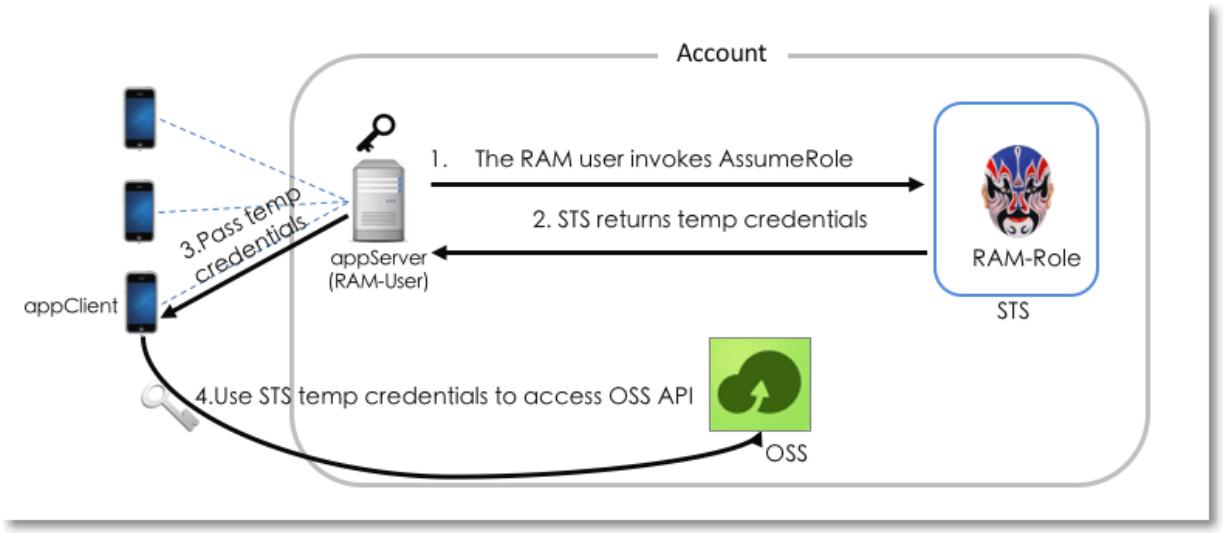
2. Account A adds the policy AliyunOSSReadOnlyAccess to the role oss-readonly. For details, see *Permission granting in RAM*.

3. Account A creates a RAM user (here, the RAM user is named appserver) for the appServer and:
   - Creates an AK for the RAM user.
   - Grants the RAM user (appserver) the permission to call the STS AssumeRole interface by attaching the AliyunSTSAssumeRoleAccess system policy to it.

Get and pass the role token

The procedure for an appClient to get and use a role token to call the OSS API is illustrated in the following figure.

Figure 4-2: Get and pass the role token



The procedure is as follows:

1. The appServer uses the AK of the RAM user (appserver) to call STS *AssumeRole* API. An example command of using aliyuncli to call AssumeRole API is as follows:

> **Note:**
> The AK for the appServer must be configured. The AK for Account A is not allowed.

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::11223344:role/oss-
readonly --RoleSessionName client-001
 {
     "AssumedRoleUser": {
         "AssumedRoleId": "391578752573972854:client-001",
         "Arn": "acs:ram::11223344:role/oss-readonly/client-001"
     },
     "Credentials": {
         "AccessKeySecret": "93ci2umK1QKNEja6WGqi1Ba7Q2Fv9P
wxZqtVF2VynUvz",
```

```
        "SecurityToken": "CAES6AIIARKAAUiwSHpkD3GXRMQk9stDr3YSVbyG
qanqkS+fPlEEkjZ+dlgFnGdCI2PV93jksole8ijH8dHJrHRA5JA1YCGsfX5hrzcNM3
7Vr4eVdWFVQhoCw0DXBpHv//ZcITp+ELRr4MHsnyGiErnDsXLkI7q/sbuWg6PACZ
/jzQfEWQb/f7Y1Gh1TVFMuRjEzR2pza1hUamszOGRCWTZZeEp0WEFaayISMz
kxNTc4NzUyNTczOTcyODU0KgpjbGllbnQtMDAxMKT+lIHBKjoGUnNhTUQ1QkoK
ATEaRQoFQWxsb3cSGwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aAwoBKhIfCg5S
ZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaAwoBKkoFNDMyNzRSBTI2ODQyWg9B
c3N1bWVkUm9sZVVzZXJgAGoSMzkxNTc4NzUyNTczOTcyODU0cgllY3MtYWRt
aW544Mbewo/26AE=",
        "Expiration": "2016-01-13T15:02:37Z",
        "AccessKeyId": "STS.F13GjskXTjk38dBY6YxJtXAZk"
    },
    "RequestId": "E1779AAB-E7AF-47D6-A9A4-53128708B6CE"
}
```

Restrict STS token permissions

1. · The Policy parameter is not specified when the preceding AssumeRole is called, indicating that the STS token has all permissions of oss-readonly.
   · You can use the Policy parameter to further restrict the permissions of the STS token, for example, to allow access to `sample-bucket/2015/01/01/*.jpg`. Example:

```
$ aliyuncli sts AssumeRole --RoleArn acs:ram::11223344:role/oss
-readonly --RoleSessionName client-002 --Policy "{\"Version\":
\"1\", \"Statement\": [{\"Effect\":\"Allow\", \"Action\":\"oss:
GetObject\", \"Resource\":\"acs:oss:*:*:sample-bucket/2015/01/01/
*.jpg\"}]}"
{
   "AssumedRoleUser": {
       "AssumedRoleId": "391578752573972854:client-002",
       "Arn": "acs:ram::11223344:role/oss-readonly/client-002"
   },
   "Credentials": {
       "AccessKeySecret": "28Co5Vyx2XhtTqj3RJgdud4ntyzrSN
dUvNygAj7xEMow",
       "SecurityToken": "CAESnQMIARKAASJgnzMzlXVyJn4KI+FsysaIpTGm
8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU78Fkszx
hnQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4
NzUyNTczOTcyODU0KgpjbGllbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEa
egoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDwoNb3NzOkdldE9i
amVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoq
Oio6c2FtcGxlLWJ1Y2tldC8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4
NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1Nzg3NTI1NzM5NzI4NTRyCWVj
cy1hZG1pbnjgxt7Cj/boAQ==",
       "Expiration": "2016-01-13T15:03:39Z",
       "AccessKeyId": "STS.FJ6EMcS1JLZgAcBJSTDG1Z4CE"
   },
   "RequestId": "98835D9B-86E5-4BB5-A6DF-9D3156ABA567"
}
```

   In addition:

   · The default validity period of the STS token is 3600 seconds (maximum limit). You can use the DurationSeconds parameter to limit the STS token expiration time.

2. The appServer retrieves and parses the credentials.
   - The appServer retrieves the AccessKeyId, AccessKeySecret, and SecurityToken from the credentials returned by the AssumeRole API.
   - The STS token validity period is determined. If the application requires a longer validity period, the appServer must re-issue a new STS token, for example, issue one STS token every 1800 seconds.
3. The appServer securely transmits the STS token to the app (appClient).
4. The app (appClient) uses the STS token to directly access the Alibaba Cloud service (such as OSS) API. The operation commands for aliyuncli to use an STS token to access an OSS object are as follows (here, an STS token is issued to client-002):

```
Configure STS token syntax: aliyuncli oss Config --host --accessid
 --accesskey --sts_token
$ aliyuncli oss Config --host oss.aliyuncs.com --accessid STS.
FJ6EMcS1JLZgAcBJSTDG1Z4CE --accesskey 28Co5Vyx2XhtTqj3RJgdud4ntyzrSN
dUvNygAj7xEMow --sts_token CAESnQMIARKAASJgnzMzlXVyJn4KI+FsysaIpTGm
8ns8Y74HVEj0pOevO8ZWXrnnkz4a4rBEPBAdFkh3197GUsprujsiU78Fkszx
hnQPKkQKcyvPihoXqKvuukrQ/Uoudk31KAJEz5o2EjlNUREcxWjRDRSISMzkxNTc4
NzUyNTczOTcyODU0KgpjbGllbnQtMDAxMKmZxIHBKjoGUnNhTUQ1Qn8KATEa
egoFQWxsb3cSJwoMQWN0aW9uRXF1YWxzEgZBY3Rpb24aDwoNb3NzOkdldE9i
amVjdBJICg5SZXNvdXJjZUVxdWFscxIIUmVzb3VyY2UaLAoqYWNzOm9zczoq
Oio6c2FtcGxlLWJ1Y2tldC8yMDE1LzAxLzAxLyouanBnSgU0MzI3NFIFMjY4
NDJaD0Fzc3VtZWRSb2xlVXNlcmAAahIzOTE1Nzg3NTI1NzM5NzI4NTRyCWVj
cy1hZG1pbnjgxt7Cj/boAQ==
Access OSS objects
$ aliyuncli oss Get oss://sample-bucket/2015/01/01/grass.jpg grass.
jpg
```

More references

For more references, see the following topics:

- *Set up direct data transfer for mobile apps*
- *Permission control*
- *Set up data callback for mobile apps*
- *STS temporary access authorization*

4.3 Cross-account resource authorization and access

This topic describes how to use RAM roles to perform cross-account resource authorization and access.

Scenario description

AccountA and AccountB represent two different enterprises (EnterpriseA and EnterpriseB, respectively). EnterpriseA has bought cloud resources (such as ECS instances, RDS instances, SLB instances, and OSS buckets) to support its business. In detail:

- EnterpriseA wants to focus on its business system, and delegate the tasks such as cloud resource operation and maintenance, monitoring, and management to EnterpriseB.
- EnterpriseB wants to further delegate those tasks to one or more of its employees . It also wants to precisely control the operations that its employees perform on EnterpriseA's cloud resources.
- If EnterpriseA or EnterpriseB terminates the preceding delegation, EnterpriseA can revoke the permissions of EnterpriseB at any time.

Requirement analysis

The requirements of the preceding scenario are analyzed as follows:

- Authorization between the two Alibaba Cloud accounts (AccountA and AccountB) is needed. AccountA is the resource owner and wants to grant AccountB the corresponding permissions to perform operations on its resources.
- AccountB wants to further grant the permissions to its sub-users (employees or applications). If an employee of AccountB joins or leaves EnterpriseB, AccountA does not have to make any changes to the permissions.
- If EnterpriseA or EnterpriseB terminates the delegation, AccountA can revoke the permissions of AccountB at any time.

Solution

Use RAM roles to perform cross-account authorization and resource access.

- AccountA creates a role in RAM, grants the corresponding permissions to the role, and allows AccountB to use this role.

  For details, see *Cross-account authorization*.

- If the employees (that is, RAM users) under AccountB need to use this role, AccountB can independently control the permissions granted to them. RAM users under AccountB can use the role to perform operations on the cloud resources of AccountA.

  For details, see *Cross-account resource access*.

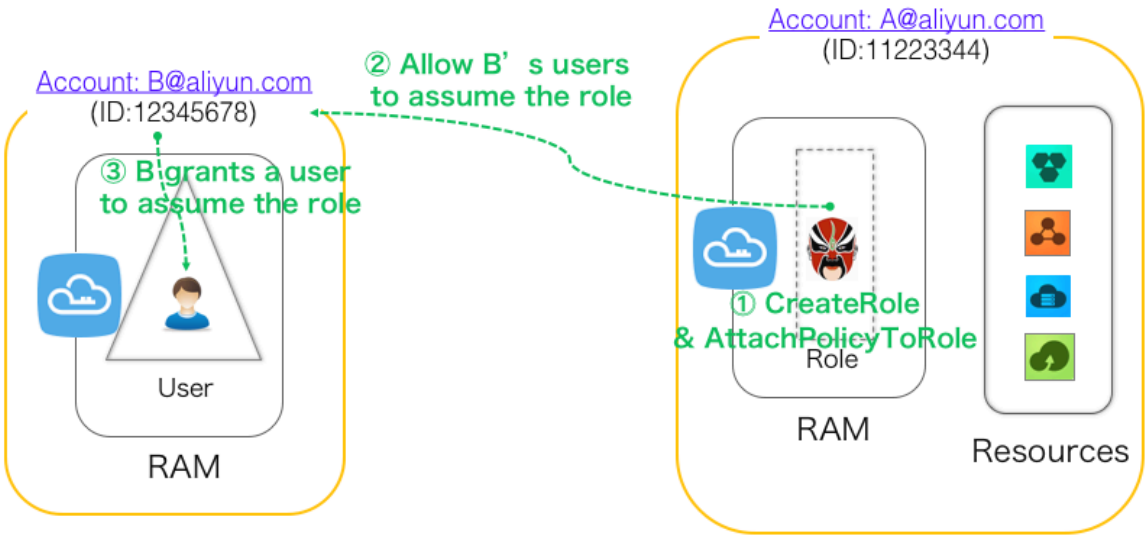
- If EnterpriseA or EnterpriseB terminates the delegation, AccountA can revoke the permissions of AccountB, thereby forcing all RAM users under AccountB (that is, all employees at EnterpriseB) to lose permissions to use this role.

  For details, see *Undo cross-account authorization*.

Cross-account authorization

The following figure shows how to use RAM roles to achieve cross-account authorization. In this example, EnterpriseA (AccountID=11223344, alias: company-a) needs to grant ECS operation permissions to the employees of EnterpriseB (AccountID=12345678, alias: company-b).

Figure 4-3: Cross-account authorization



The procedure is as follows:

1. AccountA creates a RAM role (here, the role is named ecs-admin) and selects Other Alibaba Cloud Account (AccountB: 12345678) as a trusted account, to allow the

RAM users under AccountB to assume this role. For more information, see *Manage RAM roles*.

After creating the role, AccountA can get the role information on the role details page.

- In this example, the role's Alibaba Cloud Resource Name (ARN) is:

```
acs:ram::11223344:role/ecs-admin
```

- The role's trust policy (whereby only the users under AccountB can assume this role) is as follows:

```
{
"Statement": [
{
 "Action": "sts:AssumeRole",
 "Effect": "Allow",
 "Principal": {
   "RAM": [
     "acs:ram::12345678:root"
   ]
 }
}
],
"Version": "1"
}
```

2. AccountA attaches the AliyunECSFullAccess system policy to the user role ecs-admin. For details, see *Permission granting in RAM*.
3. AccountB creates a RAM user for its employee (here, the RAM user name is Alice) and:
   - Sets a logon password (here, the logon password is 123456) for the RAM user.
   - Grants the RAM user the permission to call the STS AssumeRole interface by attaching the AliyunSTSAssumeRoleAccess system policy to it.

Cross-account resource access

RAM user Alice under AccountB wants to access AccountA's ECS resources through the Alibaba Cloud console. The procedure is as follows:

1. The RAM user (Alice) under AccountB logs on to the Alibaba Cloud console.

   Note that in actual scenarios, each RAM user must enter AccountAlias (company-b), and a valid RAM User Name and password.

2. The RAM user (Alice) under AccountB goes to Switch Role.

   To do so, in the upper right corner of the console, rest the pointer on the user icon and click Switch Role to open the Switch Role page. Enter Enterprise Alias (company-a) and Role Name (ecs-admin) to switch the role.
3. After completing the preceding steps, RAM user Alice of AccountB can perform operations on the ECS resources of AccountA.

Revocation of cross-account authorization

If AccountA wants to revoke the permission of the role ecs-admin from AccountB, the procedure is as follows:

1. AccountA logs on to the RAM console, finds the role ecs-admin on the RAM Roles page, click the role name, and then click the Trust Policy Management tab.
2. On the Trust Policy Management tab page, AccountA finds and deletes `acs:ram::12345678:root`.

    Note:
   AccountA can also revoke the permission of the role ecs-admin from AccountB by deleting the ecs-admin role on the RAM Roles page. However, the role cannot have any policies attached to it before it is deleted.

4.4 Dynamic identity and permission management of cloud applications

Scenario description

An enterprise has bought ECS instances and wants to deploy its applications in ECS . The applications require AccessKeys (AKs) to access other Alibaba Cloud APIs, for example, read the data objects in OSS buckets. To maintain account security, the applications cannot use the Alibaba Cloud account AK. Instead, the enterprise needs to create RAM users for the applications and grant the RAM users appropriate permissions. The applications can call other Alibaba Cloud APIs by using the AKs of the RAM users.

Requirement analysis

To grant the applications access to other Alibaba Cloud APIs, the enterprise can embed the AKs directly into the code, or save the AKs in the configuration files of the applications. However, the following issues occur:

1. AK disclosure. If the AKs exist in the ECS instances in plaintext, they can be mistakenly disclosed due to a snapshot, an image, or a shared image instance.
2. O&M complexity. If the AKs are changed (for example, due to AK rotation or user identity switching), all instances and images need to be updated and redeployed because the AKs exist in the ECS instances. This greatly increases the complexity of managing instances and images.

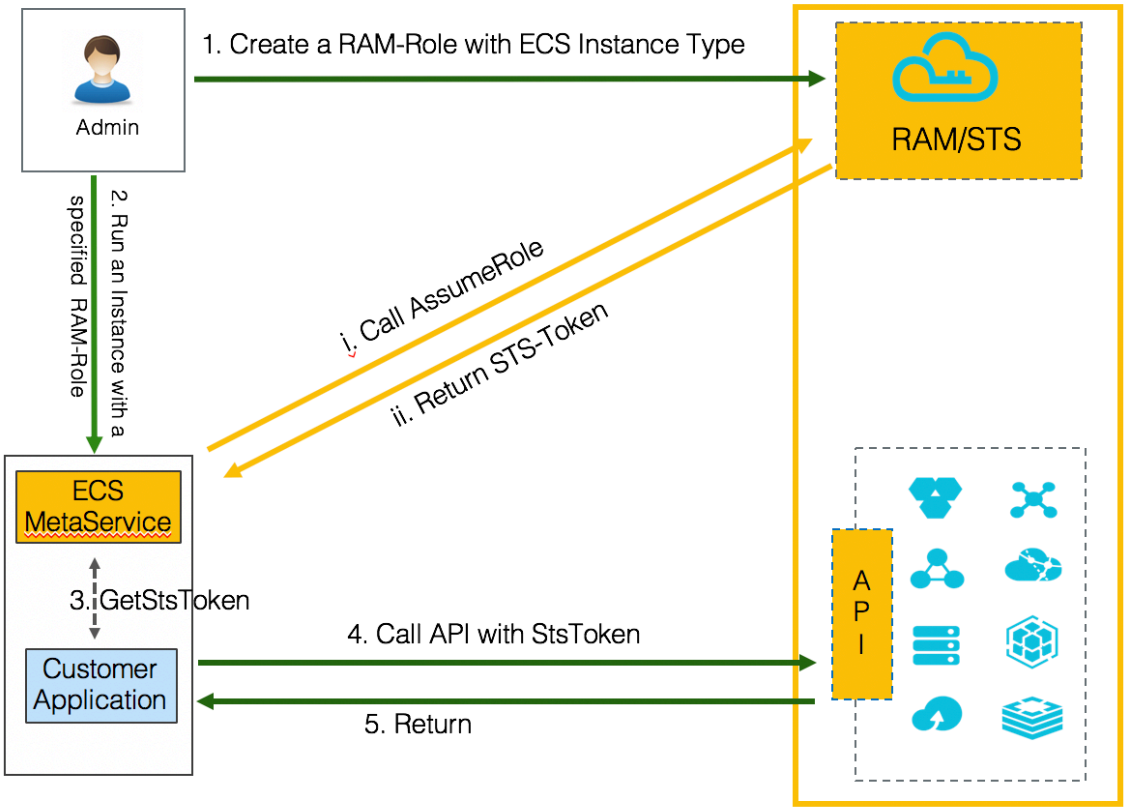
Solution

A solution to the scenario is to combine the ECS service with the access control function provided by RAM. Specifically, the administrator creates a RAM role for each ECS instance (that is, the operating environment of the application) and grants each RAM role appropriate permissions. The applications can use the dynamic STS token of the corresponding RAM role to call other Alibaba Cloud APIs. This dynamic identity and permission management method can completely solve the problems of AK disclosure and O&M complexity.

Basic concept

Figure 1 shows how the solution works.

Figure 4-4: Figure 1



1. The administrator creates an ECS instance RAM role in the RAM console and attaches appropriate policies to the RAM role.

   ECS instance RAM role: It is a type of RAM service role that is created by customers and used by the ECS instances of the customers after authorization.

2. The administrator creates an ECS instance and configures the ECS instance by using the RAM role created in the preceding step.

   When the ECS service receives the request of creating an instance:

   - (i) The ECS service calls AssumeRole according to the RAM role configured for the ECS instance, accesses the STS service, and requests a STS token for the RAM role.
   - (ii) The STS service verifies the identity of the ECS service and the policies attached to the RAM role. If the verification succeeds, a STS token is issued. Otherwise, the request is denied. Upon obtaining the STS token, the ECS service

provides it to the applications deployed in the ECS instances through the Metadata service. The STS token usually expires after one hour. The ECS service automatically refreshes the STS token before it expires.

For detailed operations, see *Use the instance RAM role in the console* or *Use the instance RAM role by calling APIs*.

3. The applications get the STS token.

   The applications in the ECS instances need to get the STS token by accessing the ECS Metadata service. For example, the following command can be used in Linux to obtain metadata information such as the STS token and its validity period:

   ```
   $ curl http://100.100.100.200/latest/meta-data/ram/security-credentials/<roleName>
   ```

4. The applications use the STS token to call Alibaba Cloud APIs.

   > **Note:**
   > If the applications use Alibaba Cloud SDK, the Alibaba Cloud SDK can get the STS token of the RAM role corresponding to the ECS instance from the ECS Metadata service, and the developers do not need to configure any AK-related sensitive information in the SDK. For more information, see *Configure RamRole to achieve non-AK access to ECS instances*.

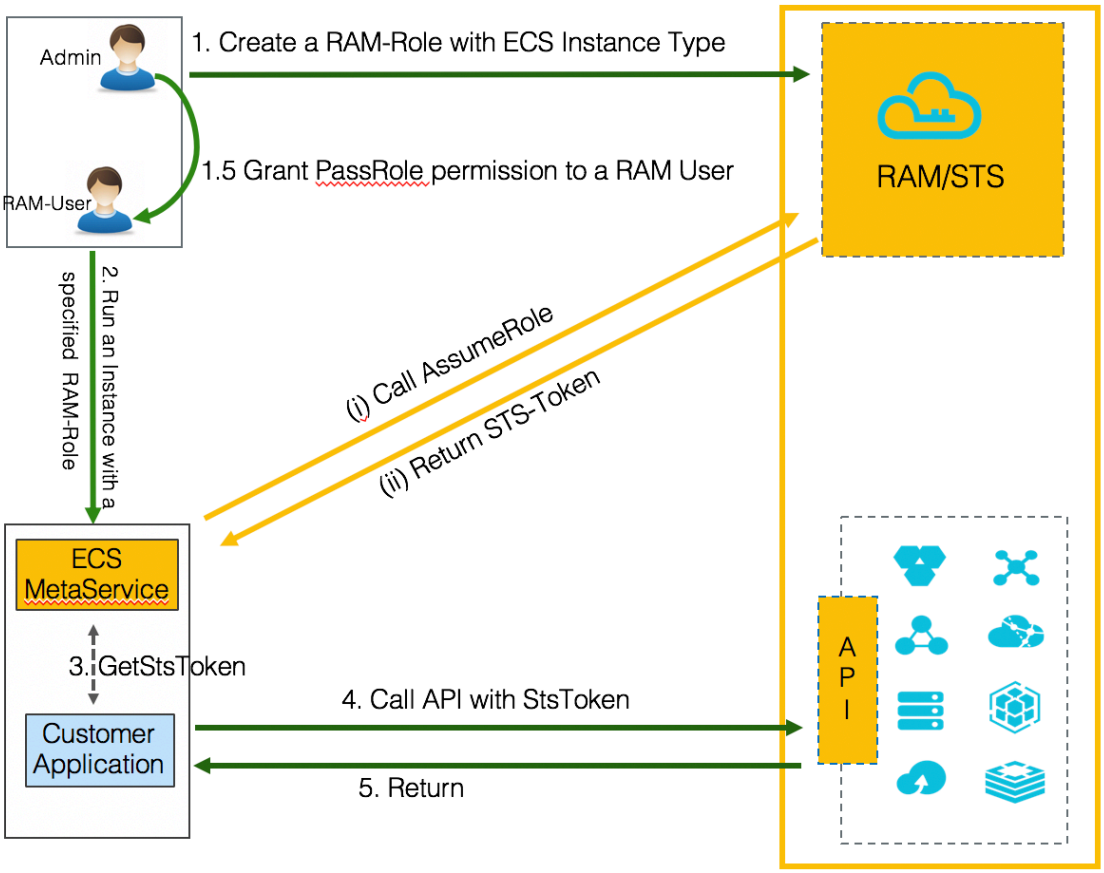
5. The applications can call Alibaba Cloud APIs when the STS token is within the validity period and has corresponding permissions. If the STS token expires, a new one needs to be obtained from the ECS Metadata service. If the STS token does not have corresponding permissions, the administrator needs to attach related policies to the RAM role. After the policies attached to the RAM role are updated, the permissions associated with the STS token take effect immediately and the user does not need to restart the ECS instance.

Supplementary scenario: separate administrators and operators

In Figure 1, the administrator acts as both the permission grantor and the ECS instance operator. However, for many corporate customers, the permission grantor and the ECS instance operator are usually different RAM users. Different people take different responsibilities.

To deal with the scenario of separate administrators and operators, we expand Figure 1 and get Figure 2.

Figure 4-5: Figure 2



Before a RAM user (for example, a RAM user that only has access to ECS and is not a RAM permission administrator) creates an ECS instance and configures the RAM role , he or she must be granted the PassRole permission of this RAM role. The ECS service runs force check to verify that the RAM user has the ram:PassRole permission of this RAM role. If the RAM user does not pass the permission check, the ECS instance cannot be created. This ensures that only authorized users can configure RAM roles for ECS instances, thus avoiding the abuse of RAM role privileges.

Except Step 1.5, the other steps in Figure 2 are the same as those in Figure 1.

In Step 1.5, the administrator grants the PassRole permission to the operator.

The administrator can create a custom policy in the RAM console by using the following sample (The *rolename* must be replaced with the RAM role name.), and then attach this custom policy to the operator:

```
{
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ram:PassRole",
      "Resource": "acs:ram:*:*:role/<rolename>"
    }
  ],
  "Version": "1"
}
```

Now you have learned the concepts and technical principles of the ECS instance RAM role. Similar access control functions through RAM roles are also provided by other Alibaba Cloud services, such as Function Compute and MaxCompute, to help customers solve the problem of identity and AK management on the cloud.

4.5 Use a local enterprise account to log on to Alibaba Cloud

Scenario description

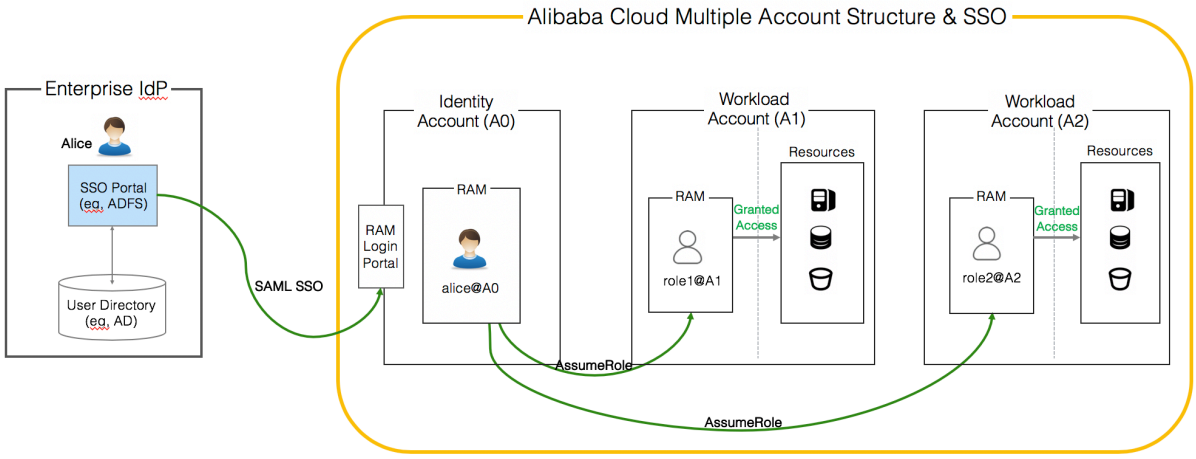
EnterpriseA has two departments that use Alibaba Cloud resources. Each department has its own Alibaba Cloud account (named as A1 and A2). EnterpriseA also has its own domain account system (Microsoft Active Directory (AD) and Active Directory Federation Services (AD FS)) and has strict requirements on identity access and security management. Specifically, it requires that all operations on Alibaba Cloud pass identity authentication through its domain account system. EnterpriseA also prohibits all employees from using independent accounts and passwords to access the cloud resources. Therefore, EnterpriseA wants to integrate its Alibaba Cloud RAM users with its local domain account system, so that all employees must use their local domain accounts to log on to Alibaba Cloud before they can access the authorized cloud resources.

Solution

Here, EnterpriseA distinguishes the accounts A1 and A2 as Workload Accounts (the account has purchased cloud resources such as virtual machines, networks, databases, or storage resources). To resolve its problem, EnterpriseA must first create a separate Identity Account, whereby only RAM users are created under the account.

Then, EnterpriseA can use the Identity Account as a service provider and integrate it with the local Identity Provider (IdP) to achieve Single Sign On (SSO). Then, EnterpriseA can use the cross-account access function provided by Alibaba Cloud through RAM roles to authorize its RAM users (employees) access to the resources under accounts A1 and A2.

Figure 4-6: Basic concept



Procedure

1. Register a new Alibaba Cloud account and use it as an Identity Account (A0). A0 is used to resolve issues concerning user synchronization and SSO.
2. Use the account A0 to log on to the RAM console and configure SSO.
3. In the AD FS of the enterprise, add A0 as a service provider.
4. Synchronize local domain users to A0: Synchronize local domain users who need to access the cloud resources to RAM.
5. Use the Workload Account A1 to log on to the RAM console, create a cross-account RAM role (RAM role 1), attach required policies to RAM role 1, and set A0 as the trusted Alibaba Cloud account.
6. Use the Workload Account A2 to log on to the RAM console, create a cross-account RAM role (RAM role 2), attach required policies to RAM role 2, and set A0 as the trusted Alibaba Cloud account.
7. Grant the RAM users under the Identity Account A0 the permission to assume RAM role 1 or RAM role 2.