

Alibaba Cloud Resource Access Management

User Guide

Issue: 20190429

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 <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

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

Legal disclaimer.....	I
Generic conventions.....	I
1 Overview.....	1
2 Identity management.....	3
2.1 User management.....	3
2.1.1 RAM users.....	3
2.1.2 RAM user groups.....	7
2.2 Logon security settings.....	9
2.2.1 Security settings.....	9
2.2.2 Domain name management.....	9
2.3 RAM roles and identities.....	11
2.3.1 RAM roles.....	11
2.3.2 RAM role management.....	15
3 Identity integration.....	21
3.1 SSO overview.....	21
3.2 Application scenarios of SSO.....	23
3.3 User-based SSO.....	24
3.3.1 User-based SSO overview.....	24
3.3.2 Configure the SAML for user-based SSO.....	26
3.3.3 Configure the SAML of an IdP during user-based SSO.....	28
3.3.4 Implement user-based SSO by using AD FS.....	29
3.4 Role-based SSO (beta version).....	37
3.4.1 Role-based SSO overview.....	37
3.4.2 Configure the SAML for role-based SSO.....	40
3.4.3 Configure the SAML of an IdP during role-based SSO.....	41
3.4.4 SAML assertions for role-based SSO.....	42
3.4.5 Implement role-based SSO by using AD FS.....	45
3.4.6 Implement role-based SSO by using Azure Active Directory.....	58
4 Permission management.....	74
4.1 Policy overview.....	74
4.2 Policy management.....	75
4.3 Permission granting.....	78
4.3.1 Permission model overview.....	78
4.3.2 Permission granting in RAM.....	79
4.4 Policy language.....	81
4.4.1 Policy elements.....	81
4.4.2 Policy structure and syntax.....	86
4.4.3 Policy example.....	89
4.5 Permission check rules.....	90

5 Scenarios.....	94
5.1 User management and access control.....	94
5.2 Grant temporary permissions to mobile apps.....	95
5.3 Cross-account resource authorization and access.....	101
5.4 Dynamic identity and permission management of cloud applications.....	104
5.5 Use an externally authorized account to log on to Alibaba Cloud.....	108

1 Overview

This topic lists the features and application scenarios of RAM.

Features

Identity management

- [RAM users](#)
- [RAM user groups](#)
- [RAM roles](#)
- [RAM role management](#)

Identity integration

- [Application scenarios of SSO](#)
- [SSO overview](#)

User-based SSO

- [User-based SSO overview](#)
- [Configure the SAML for user-based SSO](#)
- [Configure the SAML of an IdP during user-based SSO](#)
- [Implement user-based SSO by using AD FS](#)

Role-based SSO

- [Role-based SSO overview](#)
- [SAML assertions for role-based SSO](#)
- [Configure the SAML for role-based SSO](#)
- [Configure the SAML of an IdP during role-based SSO](#)
- [Implement role-based SSO by using AD FS](#)

Policy management

- [Policy management](#)
- [Permission granting in RAM](#)
- [Policy elements](#)
- [Policy structure and syntax](#)
- [Permission check rules](#)

Application scenarios

- *User management and access control*
- *Grant temporary permissions to mobile apps*
- *Cross-account resource authorization and access*
- *Dynamic identity and permission management of cloud applications*
- *Use an externally authorized account to log on to Alibaba Cloud*

2 Identity management

2.1 User management

2.1.1 RAM users

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

Before creating a RAM user

Log on to the [RAM console](#).

Create a RAM user

1. In the RAM console, click Identities and choose Users > Create User.
2. Enter the Logon Name and Display Name.



Note:

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 is automatically created for the user.

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 and click the target RAM 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 page, you can change the user name and 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, and click the target RAM 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 the following actions:

- 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 the standard user name and password method.

1. When you need to modify the console logon settings, make sure that you have selected Required for Enable MFA on the Modify Logon Settings page.
2. After the user logs on to the console, the MFA device association process is prompted. The user can follow the process to complete the MFA device association.

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 for a user who needs to call APIs, follow these steps:

1. In the RAM console, click Users and click the target RAM 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 AccessKey information and save it for later use.



Note:

- The AccessKey Secret is displayed only once during its initial creation. Currently, only the AccessKey ID, status, the latest time when the AccessKey Secret is used, and the creation time can be queried.

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

Disable an AccessKey.

In the Access Keys area, you can:

- Click Disable to disable the AccessKey.
- Click Enable to enable the AccessKey.

Delete an AccessKey.



Notice:

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

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

Log on to the console as a RAM user

The RAM user logon account is in User Principal Name (UPN) format, 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 either of the following methods:

- UPN format: <\$username>@<\$AccountAlias>.onaliyun.com



Note:

The <\$AccountAlias>.onaliyun.com is the default domain name. For more information, see [Domain name management](#).

- <\$username>@<\$AccountAlias>

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

The logon link for RAM users is <https://signin.alibabacloud.com/login.htm>.



Note:

You can also find the logon link on the Overview page after you log on to the [RAM console](#).

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 RAM user name.
2. Click Add Permissions. On the displayed Add Permissions page, the target RAM user name is entered automatically.
3. Select the policy that you want to attach to the RAM user and then click OK.

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 and select the target RAM user name.
2. Click Delete on the right.
3. In the displayed dialog box, click OK.

What to do next

- You can add a RAM user to one or more user groups and grant permissions to the group as needed. For more information, see [RAM user groups](#).
- You can attach one or more policies to a RAM user to allow the user to access resources. For more information, see [Permission granting in RAM](#).

2.1.2 RAM 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.

Advantages

Adding RAM users to user groups will bring the following benefits:

- If the responsibilities of a user change, you only need to move the user to a RAM user group with the appropriate permissions. This action does not affect other RAM users.
- If the responsibilities of a user group change, you only need to modify the policy attached to the RAM user group. Changes to the policy apply to all RAM users in the group.

Before creating a RAM user group

Log on to the [RAM console](#).

Create a RAM user group

1. In the RAM console, click **Identities** and choose **Groups > Create Group**.
2. Enter the **Group Name**, **Display Name**, and **Note**, 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.
 - To add a group member, click **Add Group Members**, select the target user (or enter keywords to search for a specific user), and click **Ok**.



Note:

You can click "X" to clear your selection.

- To remove a member from a group, select the target user, and click **Remove from Group**.

Rename a user group

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 **Modify Basic Information**.
3. Enter the **Display Name** and click **OK**.

Delete a user group

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



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.

What to do next

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 Domain name management

Each account has a default domain. You can also set a domain alias for your account. Specifically, you can customize the logon name suffix through the domain name

management function. Then, a RAM user can log on to the console using the default domain name or the domain alias.

Before a RAM user logs on to the console

The logon account of a RAM user must be in the User Principal Name (UPN) format, such as the logon user names on the Users page of the RAM console.

On the RAM user logon page, a RAM user can select either of the following logon methods:

- <\$username>@<\$AccountAlias>.onaliyun.com
- <\$username>@<\$AccountAlias>

RAM user logon entry

The logon entries for RAM users and Alibaba Cloud accounts are different.

The logon entry for RAM users is <https://signin.alibabacloud.com/login.htm>.



Note:

You can also find the logon link on the Overview page after you log on to the [RAM console](#).

Domain name management

Default domain name

1. Log on to the RAM console.
2. Click Identities and choose Settings > Advanced to view or modify the default domain name.
 - The format of the Default Domain is <\$AccountAlias>.onaliyun.com.
 - If you have not set an account alias, your account ID is used by default. In this case, the format of the Domain Alias is <\$AccountID>.onaliyun.com.

Domain alias

In addition to the default domain name, you can also set a domain alias for your account.

1. Log on to the RAM console.
2. Click Identities and choose Settings > Advanced to view the domain alias.
3. Click Create Domain Alias.

4. Enter a domain name.
5. Click OK.
6. Click Domain Ownership Verification.



Note:

After the domain alias is created, copy the verification code and paste the DNS TXT record on the domain purchase platform. After the setting is completed, verify the domain ownership.

What to do next

For more information about how to create a domain alias and set Single Sign On (SSO), see [Federated SSO overview](#).

For more information about how to manage a domain alias, see [Configure the SAML of an account](#).

2.3 RAM roles and identities

2.3.1 RAM roles

RAM roles are a type of identity defined in RAM that represent virtual users, and do not have specific identity authentication keys. RAM roles can be assumed by any trusted entity users through the console or by using a specific API. A trusted entity can be an Alibaba Cloud account, an Alibaba Cloud service, or an identity provider (IdP).



Note:

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

Related concepts

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

Figure 2-1: Concepts related to RAM roles

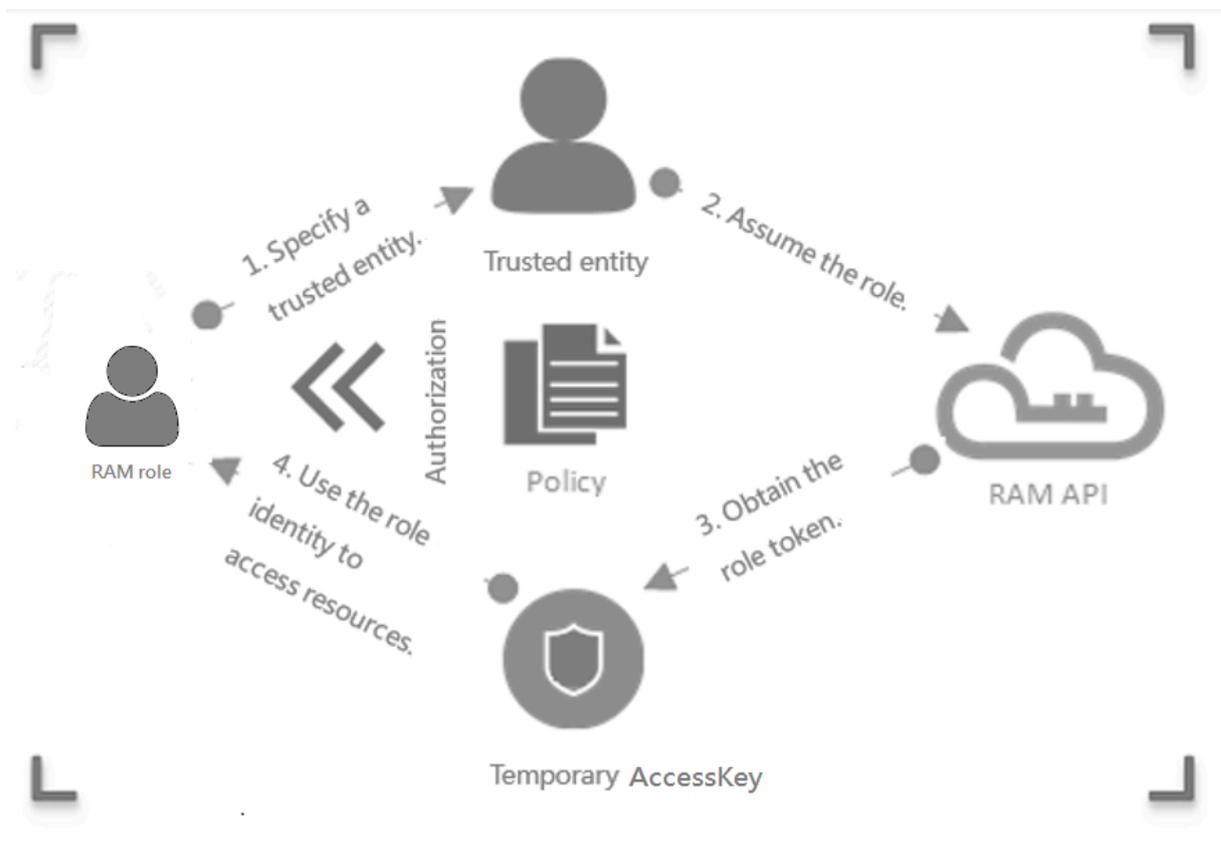


Table 2-1: Description of RAM role concepts

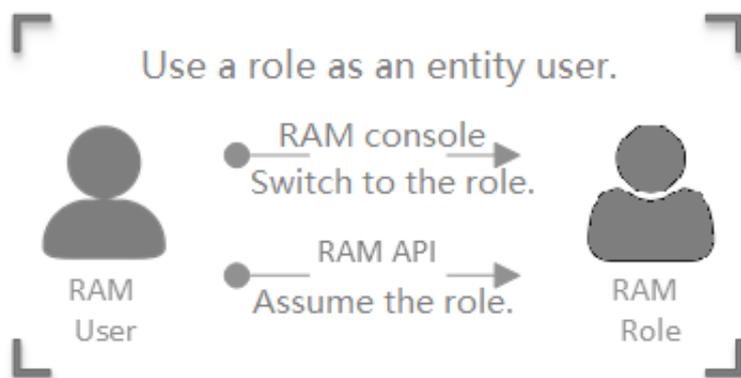
Concept	Description
ARN	<p>An ARN is the global resource identifier of a role. It is used to specify a role.</p> <ul style="list-style-type: none"> ARNs conform to Alibaba Cloud ARN naming conventions. For example, the ARN of the role devops under an account is <code>acs:ram::1234567890:12****:role/samplerole</code>. After creating a role, you can click the role name and find its ARN in the Basic Information area.

Concept	Description
Trusted entity	<p>A trusted entity is the identity of a trusted entity user who can assume a role.</p> <ul style="list-style-type: none"> · You must specify a trusted entity when creating a role. Only trusted entities can assume roles. · A trusted entity can be a trusted account, service, or IdP.
Policy	<p>A role can be attached to a set of policies. Roles that are not attached to any policy can exist, but cannot access resources.</p>
Role assuming	<p>Role assuming is the method for entity users to obtain security tokens of roles. By calling the AssumeRole API action, an entity user can obtain the security token of a role and use the token to access cloud service APIs.</p>
Identity switching	<p>Identity switching is the method by which entity users can switch from the logon identity to role identity in the RAM console.</p> <ul style="list-style-type: none"> · 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. · When the user no longer needs the role identity, the user can switch back to its logon identity.
Role token	<p>A role token is a temporary AccessKey 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 assume the role to obtain the role token. Then, the user can use the role token to call Alibaba Cloud service APIs.</p>

Instructions

RAM roles can be used only after they are assumed by trusted entity users.

Figure 2-2: Use RAM roles



The difference between RAM roles and textbook roles is as follows:

- 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).
- 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.

The difference between entity users and virtual users is as follows:

- Entity users have specific logon passwords or AccessKeys. 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.

RAM role types

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

- **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 as stand-alone applications.

- **IdP:** roles that users in an entrusted IdP can assume. Such roles are used to implement single sign-on (SSO) to Alibaba Cloud.

Application scenarios of RAM roles

- [Grant temporary permissions to mobile apps](#)
- [Cross-account resource authorization and access](#)
- [Dynamic identity and permission management of cloud applications](#)

2.3.2 RAM role management

This topic describes how to manage RAM roles. RAM roles can be assumed either in the RAM console or through APIs. After creating a RAM role, you can grant permissions to the role so that the role can access specified resources.



Note:

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

Create a RAM role

- **Create a RAM role for a trusted Alibaba Cloud Account.**
 1. Log on to the [RAM console](#).
 2. In the left-side navigation pane, choose RAM Roles.
 3. On the displayed page, click Create RAM Role.
 4. Select Alibaba Cloud Account and click Next.
 5. Enter a role name in the RAM Role Name field. You can also enter a description in the Note field. Then, select a trusted Alibaba Cloud account and click OK.
 - To create a role for RAM users under your account (for example, authorizing mobile app clients to directly operate on OSS resources), select Current Alibaba Cloud Account as the trusted account.
 - To create a role for RAM users under another account (for example, cross-account resource authorization), select Other Alibaba Cloud Account as the trusted account and enter the account ID.

- Create a RAM role for a trusted Alibaba Cloud Service.
 1. Log on to the [RAM console](#).
 2. In the left-side navigation pane, choose RAM Roles.
 3. On the displayed page, click Create RAM Role.
 4. Select Alibaba Cloud Service and click Next.
 5. Enter a role name in the RAM Role Name field. You can also enter a description in the Note field. Then, select a trusted service and click OK. Available services include:
 - **Media Transcoding Service:** You can create 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:** You can create 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:** You can create a role, configure Log Service as its trusted service, and use Log Service to assume the role and write data into OSS when you import Log Service-collected logs into OSS.
 - **API Gateway:** You can create 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:** You can create a role and use this role to authorize ECS to access your cloud resources in other cloud services.



Note:

For more information about the trusted services, see the RAM console.

- Create a RAM role for a trusted IdP.
 1. Log on to the [RAM console](#).
 2. In the left-side navigation pane, choose RAM Roles.
 3. On the displayed page, click Create RAM Role.
 4. Select IdP and click Next.
 5. Enter a role name in the RAM Role Name field. You can also enter a description in the Note field. Then, select a trusted IdP.
 6. View the conditions and click OK.

**Note:**

In the conditions, only the keyword `saml : recipient` (which is required and cannot be modified) is currently allowed. This keyword corresponds to the value of the `Recipient` attribute in the `Subject - SubjectConfirmation - SubjectConfirmationData` element of the SAML assertion. The value of the condition must be set to `https://signin.alibabacloud.com/saml-role/sso`.

Edit a RAM role

On the RAM Roles page, click the name of the role you created to view the basic information. On the Trust Policy Management tab, click Edit Trust Policy. Then, you can change the trusted entity that assumes the role by modifying the 'Principal' element in the policy. The 'Principal' element determines the entrusted entity of the role.

1. If the 'Principal' element contains a 'RAM' field, the entrusted entity is an Alibaba Cloud account, and the role can be assumed by RAM users under the entrusted account. The following is an example:

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::1234567890:12:****:root"
        ]
      }
    }
  ]
}
```

```
    ],
    " Version ": " 1 "
  }
}
```

The preceding policy indicates that the role can be assumed by any RAM user under the Alibaba Cloud account (123456789012****). If you modify the 'Principal' element as follows, the role can be assumed by the RAM user (testuser) under the Alibaba Cloud account (123456789012****):

```
    " Principal ": {
      " RAM ": [
        " acs : ram :: 1234567890 12 ****: user /
testuser "
      ]
    }
```

2. If the 'Principal' element contains a 'Service' field, the entrusted entity is an Alibaba Cloud service, and the role can be assumed by entrusted Alibaba Cloud services under the current Alibaba Cloud account. The following is an example:

```
{
  " Statement ": [
    {
      " Action ": " sts : AssumeRole ",
      " Effect ": " Allow ",
      " Principal ": {
        " Service ": [
          " ecs . aliyuncs . com "
        ]
      }
    }
  ],
  " Version ": " 1 "
}
```

The preceding policy indicates that the role can be assumed by ECS under the current Alibaba Cloud account.

3. If the 'Principal' element contains a 'Federated' field, the entrusted entity is an identity provider (IdP), and the role can be assumed by users under the entrusted IdP. The following is an example:

```
{
  " Statement ": [
    {
      " Action ": " sts : AssumeRole ",
      " Effect ": " Allow ",
      " Principal ": {
        " Federated ": [

```

```
    "acs : ram :: 1234567890 12 ****: saml -
    provider / testprovider "
  ],
  "Condition ":{
    "StringEquals ":{
      "saml : recipient ":" https :// signin .
      alibabacloud . com / saml - role / sso "
    }
  }
},
"Version " : " 1 "
}
```

The preceding policy indicates that the role can be assumed by users under the IdP (testprovider) in the current Alibaba Cloud account (123456789012****).

Use a RAM role

Roles that are created for an Alibaba Cloud Service can be assumed only by trusted cloud services, roles that are created for an Alibaba Cloud Account can be assumed by RAM users, and roles that are created for an IdP can be assumed by users under the entrusted IdP.

1. Create a RAM user and create an AccessKey or set a password for the user.
2. Attach the system policy AliyunSTSAssumeRoleAccess or an STS custom policy to authorize the RAM user.



Note:

To maintain account security, a trusted Alibaba Cloud account is not allowed to assume roles itself. Roles must instead be assumed by RAM users of the Alibaba Cloud account.

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

- Assume RAM roles in the RAM console.

If an entity user wants to assume a RAM role, the entity user must log on to the RAM console and switch their role.

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



Note:

- After switching the role, you can log on to the console as a RAM user with the new RAM role. After you log on, both the current role and identity and the logon identity are displayed in the upper-right corner of the console.
- After switching the role, you can only perform operations that are authorized to this role. The access permission of your original identity is hidden when you log on to the console.

4. Click Switch Back to Logon User to switch back to your logon identity.



Note:

After switching to the logon identity, you will obtain the original permissions and lose the permissions associated with the role.

- Assume RAM roles through APIs.

After being granted the AssumeRole permission, a RAM user can use its AccessKey to call the AssumeRole API action 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 more information about how to call the AssumeRole API action, see [AssumeRole](#).

What to do next

After creating a role, you can click Add Permissions to RAM role to grant permissions to this role. For more information, see [Permission granting in RAM](#).

3 Identity integration

3.1 SSO overview

Alibaba Cloud supports SAML 2.0-based Single Sign On (SSO, also known as identity federation). This topic introduces how to implement SSO between enterprises and Alibaba Cloud.

Terms

The following table lists some basic terms related to SAML and SSO.

Table 3-1: Terms

Term	Description
Identity Provider (IdP)	<p>Provides identity management services. IdPs are generally classified into the following types:</p> <ul style="list-style-type: none"> · 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)	<p>Uses the identity management function of an IdP to provide users with specific service applications. An SP consumes the user information provided by an IdP. In some identity systems (such as OpenID Connect) that do not comply with the SAML protocol, SP is known as relying party, which means the relying party of an IdP.</p>
Security Assertion Markup Language 2.0 (SAML 2.0)	<p>A 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 standard that enterprises can use to implement identity federation.</p>

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 SAML metadata of an IdP in a trusted way. 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.

Methods of SSO

Enterprises can implement SSO with Alibaba Cloud through SAML 2.0-based IdP (for example, AD FS). Alibaba Cloud offers the following two SAML 2.0-based SSO methods:

- **User-based SSO:** The RAM user that you can use to log on to Alibaba Cloud can be determined through a SAML assertion. After logon, you can use the RAM user to access Alibaba Cloud.

For more information, see [User based federation overview](#).

- **Role-based SSO:** The RAM role that you can use to log on to Alibaba Cloud can be determined through SAML assertions. After logon, you can use the role specified in the SAML assertion to access Alibaba Cloud.

For more information, see [Role based federation overview](#).

Comparison between role-based SSO and user-based SSO

SSO method	Supports SSO initiated by SP?	Supports SSO initiated by IdP?	Supports logon with your RAM account and password?	Supports association of one IdP and multiple Alibaba Cloud accounts?	Supports multiple IdPs?
User-based SSO	Yes	Yes	No	No	No
Role-based SSO	No	Yes	Yes	Yes	Yes



Note:

For more information, see [Application scenarios of SSO](#).

3.2 Application scenarios of SSO

This topic describes the application scenarios of two SSO methods supported by Alibaba Cloud: role-based SSO and user-based SSO.

Role-based SSO

Application scenarios:

- You do not want to create or manage users on Alibaba Cloud to avoid user synchronization and reduce costs.
- You want to implement SSO to Alibaba Cloud and manage some users on Alibaba Cloud. The users managed on Alibaba Cloud can be used to test new features of Alibaba Cloud and log on to Alibaba Cloud if your network or identity provider (IdP) encounters exceptions.
- You want to manage the operation permissions on Alibaba Cloud according to the user groups in your local IdP or a specific user attribute. Then, you can manage user permissions by grouping users in your local IdP or changing the attribute of a user.

- You have multiple Alibaba Cloud accounts and only one IdP. You want to implement SSO to multiple Alibaba Cloud accounts by configuring your IdP only once.
- You have multiple IdPs and only one Alibaba Cloud account. You want to implement SSO from multiple IdPs to one Alibaba Cloud account by configuring IdPs in the Alibaba Cloud account.
- You want to implement SSO by using the console or by calling APIs.

User-based SSO

Application scenarios:

- You want to initiate logon from Alibaba Cloud, not from your IdP.
- Some of your Alibaba Cloud services cannot be accessed by roles (that is, through STS). For more information about Alibaba Cloud services that can be accessed by roles, see [Alibaba Cloud services that work with RAM](#).
- Your IdP does not support complex configuration of attributes.
- You want to simplify IdP configuration.

3.3 User-based SSO

3.3.1 User-based SSO overview

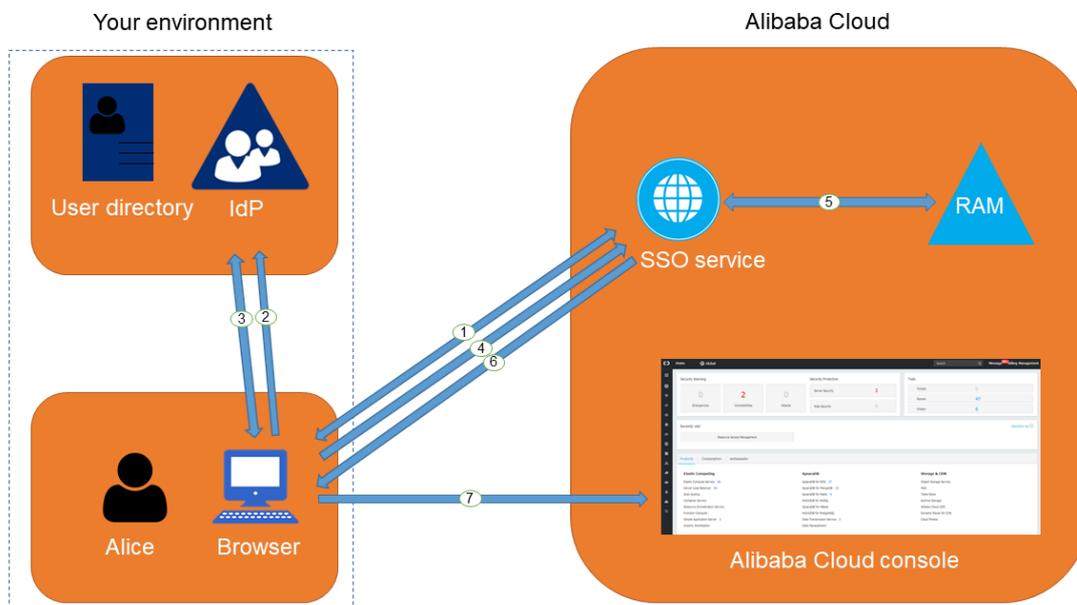
This topic describes the scenario, process, and configuration of user-based SSO.

Scenario

In scenarios where Alibaba Cloud and the identity management system of an enterprise work together to perform user-based SSO, Alibaba Cloud is the SP and the enterprise system is the IdP. User-based SSO allows an employee in the enterprise to access Alibaba Cloud as a RAM user.

User-based SSO process

Figure 3-1: Process



As shown in the figure, after the administrator configures user-based SSO, the employee (Alice) can log on to Alibaba Cloud after the following steps are completed:

1. Alice logs on to the Alibaba Cloud console through a browser, and Alibaba Cloud returns an SAML authentication request to the browser.
2. The browser forwards the SAML authentication request to the IdP.
3. The IdP prompts Alice to log on and returns an SAML response to the browser.
4. The browser forwards the SAML response to the SSO service.
5. Through the SAML mutual trust configuration, the SSO service verifies the digital signature in the SAML response to check the authenticity of the SAML assertion, and then matches the identity of the RAM user according to the value of `NameID` in the SAML assertion.
6. The SSO service returns 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 does not necessarily have to log on to Alibaba Cloud. Instead, the employee can click the link on the IdP portal to send an SAML authentication request to the IdP and access the Alibaba Cloud console.

User-based SSO configuration

Before you use user-based SSO, you must set configurations to establish trust between Alibaba Cloud and your IdP.

1. To make sure your IdP is trusted by Alibaba Cloud, you must configure the IdP in the Alibaba Cloud console.

For more information, see [Configure the SAML of an account](#).

2. To make sure Alibaba Cloud is trusted by the IdP, you must configure Alibaba Cloud as a trusted SAML SP and configure an SAML assertion in your IdP.

For more information, see [Configure the SAML of an IdP during user-based SSO](#).

3. After the IdP and Alibaba Cloud are configured, you must create RAM users to match your IdP through SDK, CLI or logging on to the RAM console.

For more information, see [RAM users](#).

The processes of configuring an SAML assertion and an SAML SP vary according to the IdP system. For more information about how to implement user-based SSO from Microsoft Active Directory Federation Service (AD FS) to Alibaba Cloud, see [Identity federation of an enterprise IdP and Alibaba Cloud](#).

3.3.2 Configure the SAML for user-based SSO

This topic describes how to configure the metadata for user-based SSO according to SAML 2.0 to establish trust between your identity provider (IdP) and Alibaba Cloud.

Set the default domain name and domain alias of an account

You can simplify SAML Single Sign On (SSO) by using a domain name or a domain alias. For more information about how to set a default domain name and a domain alias, see [Domain name management](#).

Set SAML SSO

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, choose SSO.

3. On the User-based SSO tab, click Modify next to SSO Settings.

- **Metadata File:** You can click Upload to upload the metadata file provided by your IdP.

**Note:**

The metadata file, usually in XML format, is provided by an 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 enable or disable the SSO function as needed.
 - The SSO function is disabled by default. When the SSO function is disabled, RAM users can use their passwords for logon, and all SSO settings do not take effect.
 - If you enable the SSO function, RAM users cannot use their passwords for logon. They must log on to an IdP for identity authentication. If the SSO function is disabled later, the page for logon using passwords is automatically displayed.

**Note:**

The SSO function takes effect only for the RAM users under an account.

What to do next

You can migrate or synchronize data from your IdP to Alibaba Cloud or Alibaba Cloud RAM by using either of the following methods:

- Log on to the RAM console and create RAM users that match the users in your IdP.
- Use a RAM SDK to write a program or use Alibaba Cloud command line interface (CLI) to customize a solution.

3.3.3 Configure the SAML of an IdP during user-based SSO

This topic describes how to configure the SAML of an identity provider (IdP) during user-based SSO. You can configure Alibaba Cloud as a trusted SAML service provider (SP), and configure an SAML assertion in the IdP.

Configure Alibaba Cloud as a trusted SAML SP

1. Obtain the SAML SP metadata URL from Alibaba Cloud:
 - a. Log on to the [RAM console](#).
 - b. In the left-side navigation pane, choose SSO.
 - c. On the User-based SSO tab, obtain the SAML SP metadata URL.
2. Create an SAML SP in the target IdP and configure the SAML SP 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.

Configure an SAML assertion in the IdP

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

If you configure the SAML assertion issued by the IdP, you must map the UPN of the target RAM user to the NameID in the SAML assertion.

For more information about how to configure an SAML assertion in an IdP, see [Implement user-based SSO by using AD FS](#).

3.3.4 Implement user-based SSO by using AD FS

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

Prerequisites

Microsoft AD is properly configured and the following server roles are 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.

Notes

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

Example configuration

The configuration details used in the example are 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 on-premises Microsoft AD:** `adfs . secloud . club .`
- **Domain name of the on-premises 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 / Federation Metadata / 2007 - 06 / Federation Metadata . xml
```

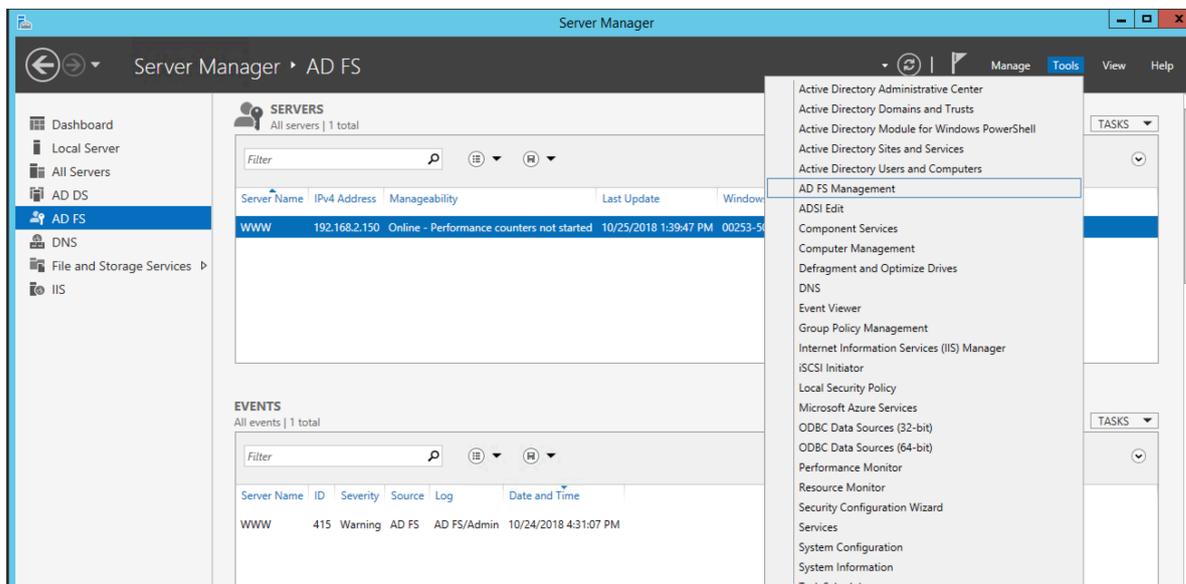
2. Download the metadata file in XML format.

3. In the RAM console, use the metadata file for SSO configuration.

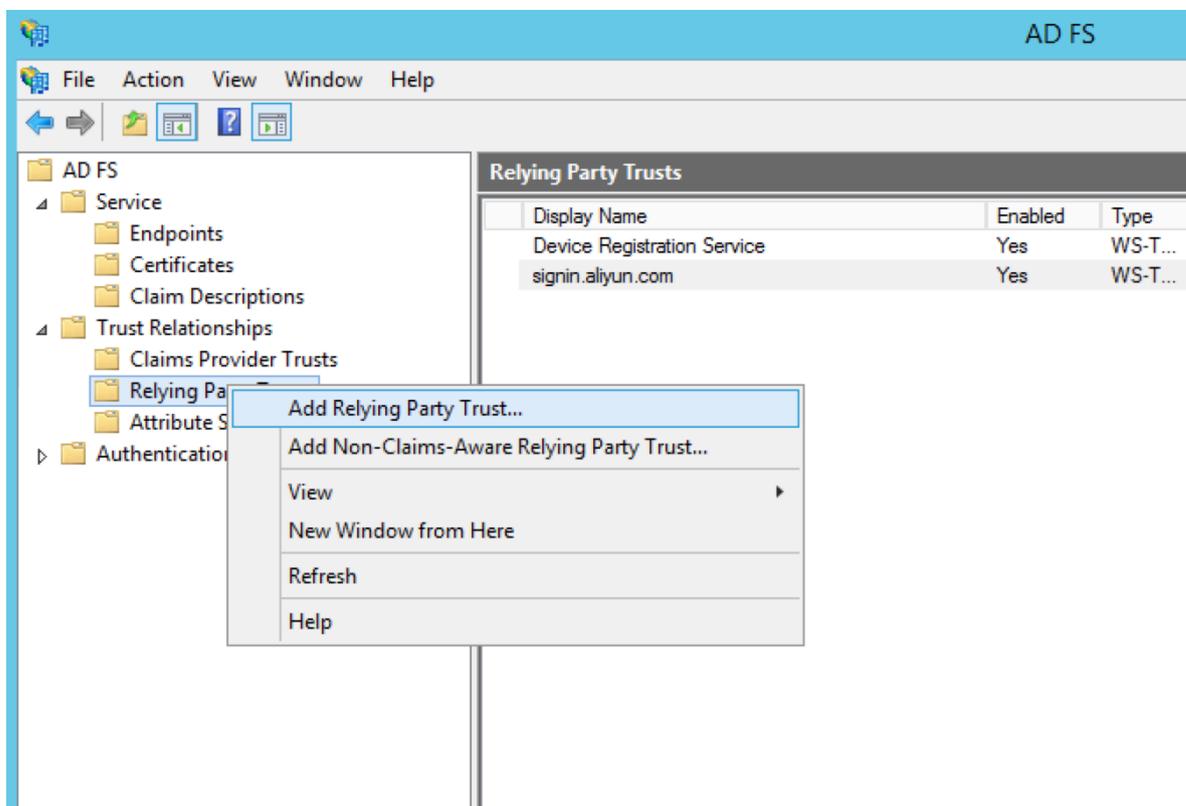
Configure Alibaba Cloud as a trusted SAML SP in AD FS

In AD FS, SAML SP is called relying party. To configure Alibaba Cloud as a trusted SP, follow these steps:

1. On the Server Manager page, choose Tools > AD 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, choose SSO in the left-side navigation pane, and click User-based SSO. You can enter the metadata URL when configuring the AD FS relying party.

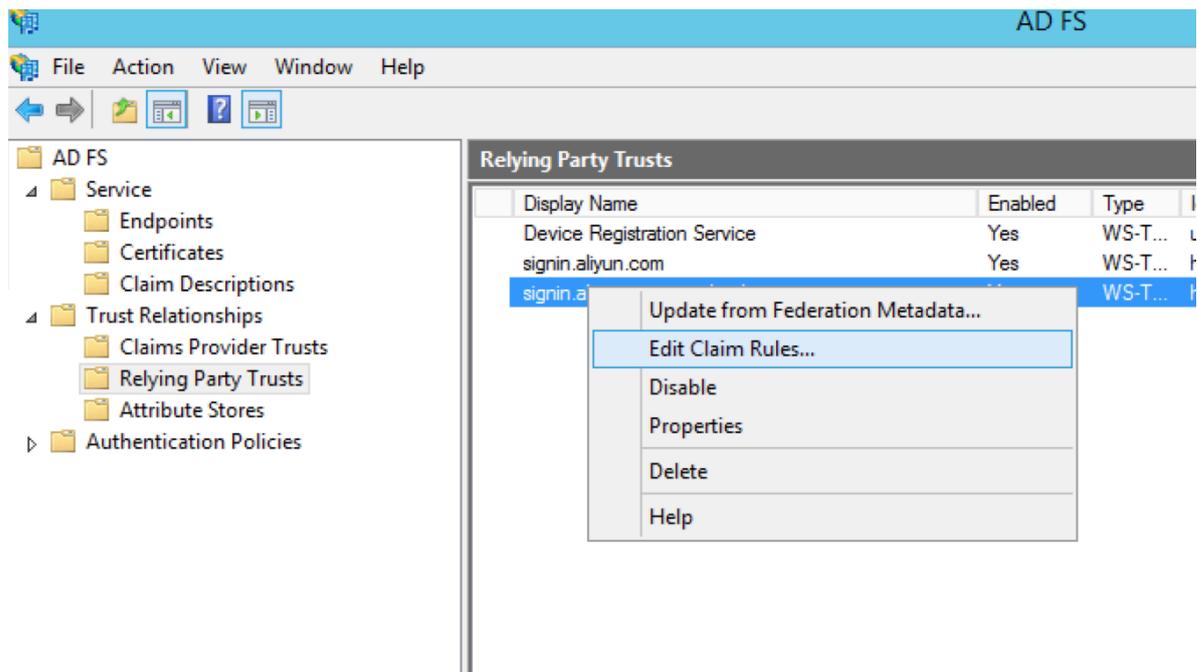
After the relying party is configured, Alibaba Cloud sends a request to authenticate the RAM user whose domain name is `secloud.onaliyun.com` to AD FS `adfs.secloud.club`. AD FS receives the request from Alibaba Cloud, authenticates the user, and sends a response to Alibaba Cloud.

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. Right-click the display name of the relying party and select Edit Claim Rules.

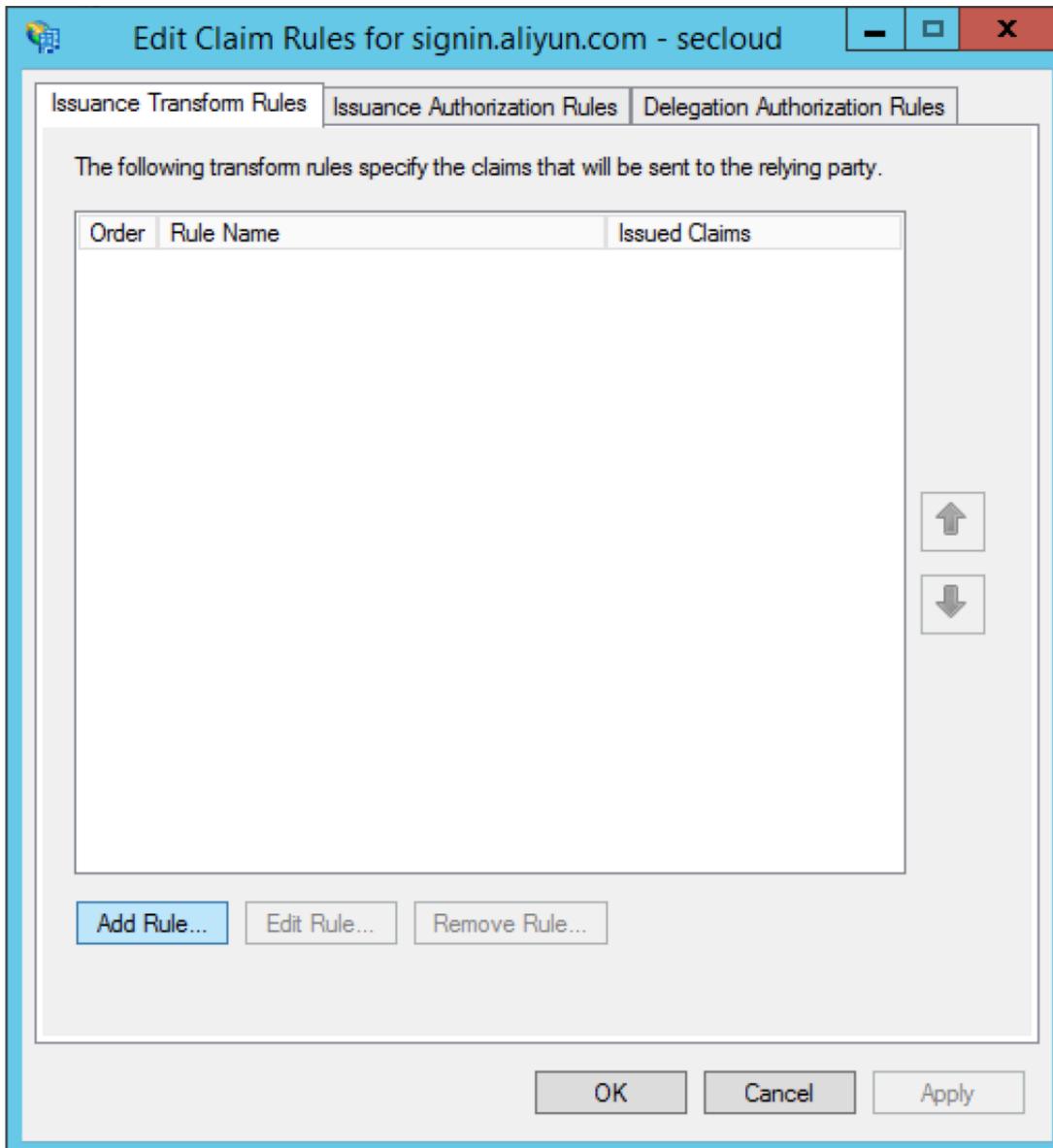


2. Click Issuance Transform Rules to add a rule.



Note:

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. From the Claim rule template drop-down list, select Transform an Incoming Claim.

Add Transform Claim Rule Wizard

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

< Previous Next > Cancel

4. Select Edit Rule.



Note:

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 more information, see [Configure the SAML for user-based SSO](#).

After the settings are completed, map the UPN to the NameID on the Edit Rule page.

Edit Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: UNP2NameID

Rule template: Transform an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

Pass through all claim values

Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

View Rule Language... OK Cancel

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 . onalinyun . 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 . onalinyun . com` .

Edit Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:
UNP2NameID

Rule template: Transform an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

Pass through all claim values

Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value: Browse...

Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix: secloud.onalinyun.com
Example: fabrikam.com

View Rule Language... OK Cancel

3.4 Role-based SSO (beta version)

3.4.1 Role-based SSO overview

This topic describes the scenario, process, and configuration of role-based SSO.

Scenario

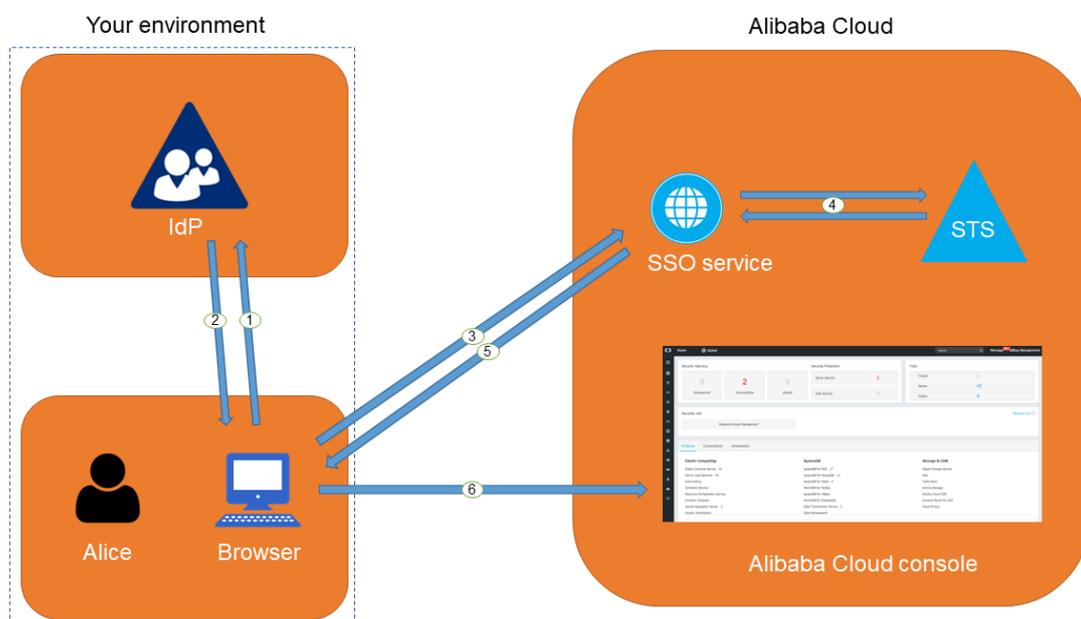
In scenarios where Alibaba Cloud and the identity management system of an enterprise work together to perform role-based SSO, Alibaba Cloud is the SP and the enterprise system is the IdP. Through role-based SSO, the enterprise can manage users in the local IdP without synchronizing users from your IdP to Alibaba Cloud, and the enterprise employee can log on to Alibaba Cloud using a specific RAM role.

Role-based SSO process

Through role-based SSO, you can access Alibaba Cloud either by logging on to the Alibaba Cloud console or by using a program.

Access Alibaba Cloud through the console

Figure 3-2: Process



As shown in the figure, after the administrator configures role-based SSO, the employee (Alice) can log on to Alibaba Cloud after the following steps are completed:

1. Alice uses the browser to select Alibaba Cloud as the target service on logon page of the IdP.

For example: If the IdP is Microsoft Active Directory Federation Service (AD FS), the log on URL will be `https://ADFSServiceName/adfs/ls/IdpInitiatedSignOn.aspx`.



Note:

Some IdPs require users to log on first and then select an SSO application that represents Alibaba Cloud.

2. The IdP generates a SAML response to the browser.
3. The browser redirects to the page of the SSO service, and forwards the SAML response.
4. The SSO service uses the SAML response to request an STS token from Alibaba Cloud STS service, and generates a URL that can log on to the Alibaba Cloud console with the STS token.



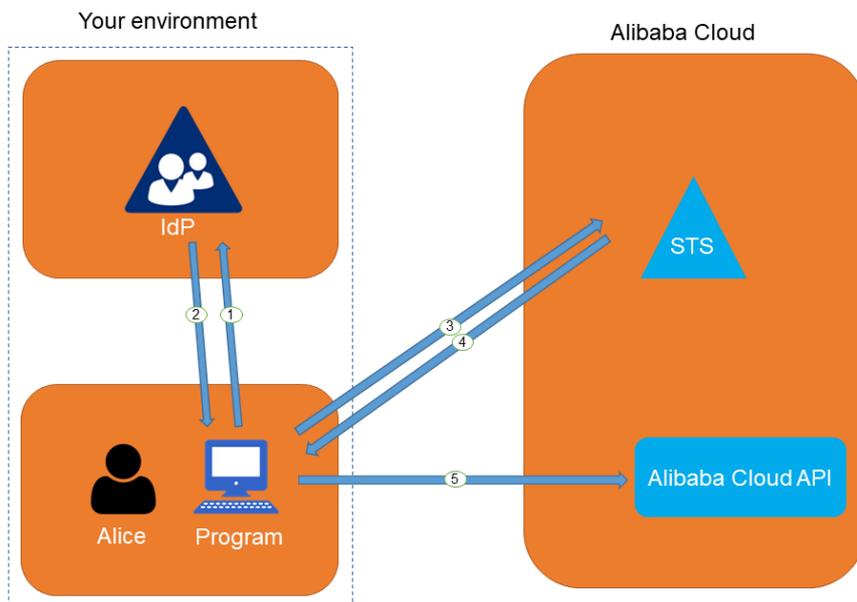
Note:

If the SAML response contains attributes that map to multiple RAM roles, the user is prompted to select a role firstly.

5. The SSO service returns the URL to the browser.
6. The browser redirects to the URL, and logs on to the Alibaba Cloud console with the specific RAM role.

Access Alibaba Cloud through a program

Figure 3-3: Process



As shown in the figure, the employee (Alice) can log on to Alibaba Cloud after the following steps are completed:

1. Alice initiates an authentication request to the IdP through a program.
2. The IdP generates a SAML response that contains the user's SAML assertion, and returns the SAML response to the program.
3. The program calls Alibaba Cloud STS service API action *AssumeRoleWithSAML*, and forwards the information including the ARN of an Alibaba Cloud identity provider, the ARN of the role to be assumed, and the SAML assertion obtained from the IdP.
4. STS service verifies the SAML assertion and returns an STS token to the program.
5. The program calls an Alibaba Cloud API action with the STS token.

Role-based SSO configuration

Before you use role-based SSO, you must set configurations to establish trust between Alibaba Cloud and your IdP.

1. To make sure your IdP is trusted by Alibaba Cloud, you must configure the IdP in the Alibaba Cloud console.

For more information, see [Configure the SAML for role-based SSO](#).

2. You must use a program or log on to the RAM console to create RAM roles and grant permissions to them.

For more information, see [RAM role management](#).

3. To make sure Alibaba Cloud is trusted by the IdP, you must configure Alibaba Cloud as a trusted SAML SP and configure SAML assertions in your IdP.

For more information, see [Configure the SAML of an IdP during role-based SSO](#).

The processes of configuring SAML assertions and an SAML SP vary according to the IdP system. For more information about how to implement role-based SSO from AD FS to Alibaba Cloud, see [Implement role-based SSO by using AD FS](#).

3.4.2 Configure the SAML for role-based SSO

This topic describes how to configure the metadata for role-based SSO according to SAML 2.0 to establish trust between your identity provider (IdP) and Alibaba Cloud.

Create an IdP in RAM

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, choose SSO.
3. On the Role-based SSO tab, click Create IdP.
4. Enter the IdP Name and Note.
5. In the Metadata File area, click Upload.



Note:

The metadata file, usually in XML format, is provided by an IdP. It contains the IdP's logon service address, the public key for verifying the SAML assertion, and the assertion format.

6. Click OK. After creating an IdP, you can view and modify basic information of the IdP:
 - Click the target IdP name to view the basic information of the IdP, including the IdP name, ARN, and the metadata file.
 - On the IdP Information page, click Modify to modify the basic information of the IdP, including the IdP name and the metadata file.



Note:

If you want to delete the IdP, click Delete.

What to do next

After creating an IdP in RAM, you must create one or more RAM roles with the trusted entity type set to IdP, to establish an association between the IdP and Alibaba Cloud.

Click **Create RAM Role** to navigate to the page for creating RAM roles. For more information about how to create a RAM role, see [RAM role management](#).

3.4.3 Configure the SAML of an IdP during role-based SSO

This topic describes how to configure the SAML of an identity provider (IdP) during role-based SSO. You can configure Alibaba Cloud as a trusted SAML service provider (SP), and configure SAML assertions in the IdP.

Configure Alibaba Cloud as a trusted SAML SP

1. Obtain the SAML SP metadata URL (`https://signin.alibabacloud.com/saml-role/sp-metadata.xml`) from Alibaba Cloud.

**Note:**

You can also log on to the RAM console and choose SSO in the left-side navigation pane. On the Role-based SSO tab, copy the URL and configure it in your IdP.

2. Download the XML file and upload it to your IdP.

**Note:**

If the XML file cannot be uploaded to the IdP, you need to configure the following parameters:

- Entity ID : `urn:alibaba:cloudcomputing:international`
- ACS URL : `https://signin.alibabacloud.com/saml-role/SSO`

3. Create an SAML SP in the target IdP and configure the SAML SP metadata URL of Alibaba Cloud.

Configure SAML assertions in the IdP

Alibaba Cloud resolves an SAML assertion to determine a RAM role. Therefore, the SAML assertion generated by the IdP must contain the necessary information of the RAM role.

For more information about SAML assertions, see [SAML assertions for role-based SSO](#).

3.4.4 SAML assertions for role-based SSO

This topic describes the mandatory attribute elements in SAML assertions issued by your identity provider (IdP) for role-based SSO.

Scenario

During SAML 2.0-based SSO, after the identity of a user is verified, your IdP generates an authentication response and sends it to Alibaba Cloud through a browser or a program. This response contains a SAML assertion that complies with the HTTP POST Binding for SAML 2.0 standard.

Alibaba Cloud uses the SAML assertion to determine the logon status and identity of the user. Therefore, the SAML assertion must contain elements that are required by Alibaba Cloud.

Common elements in SAML 2.0

- **Issuer**

The value of the **Issuer** element must match the **EntityID** in the IdP metadata file uploaded in the IdP created in Alibaba Cloud.

- **Signature**

The SAML assertion in Alibaba Cloud must be used as a signature. The **Signature** element must contain information such as the signature value and signature algorithm.

- **Subject**

The **Subject** element must contain the following sub-elements:

- Only one **NameID** sub-element. You must specify the value of **NameID** according to SAML 2.0. But note that Alibaba Cloud does not determine a logon identity according to the value of **NameID**.
- Only one **SubjectConfirmation** sub-element with a **SubjectConfirmationData** sub-element. The **SubjectConfirmationData** sub-element must contain the following attributes:
 - **NotOnOrAfter** : specifies the validity of an SAML assertion.
 - **Recipient** : Alibaba Cloud checks whether it is the recipient of the SAML assertion according to the value of the **Recipient** element. Therefore, you

must set `Recipient` to `https://signin.alibabacloud.com/saml-role/sso`.

The following is an example of the `Subject` element:

```
< Subject >
  < NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"> administrator </ NameID >

  < SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    < SubjectConfirmationData NotOnOrAfter="2019-01-01T00:01:00.000Z" Recipient="https://signin.alibabacloud.com/saml-role/sso"/>
  </ SubjectConfirmation >
</ Subject >
```

- `Conditions`

The `Conditions` element must contain an `AudienceRestriction` sub-element. The `AudienceRestriction` sub-element can contain multiple `Audience` sub-elements, and the value of an `Audience` sub-element must be `urn:alibaba:cloudcomputing:international`.

The following is an example of the `Conditions` element:

```
< Conditions >
  < AudienceRestriction >
    < Audience > urn:alibaba:cloudcomputing:international
  </ Audience >
  </ AudienceRestriction >
</ Conditions >
```

Custom elements required by Alibaba Cloud

The `AttributesStatement` element in an SAML assertion must contain the following `Attribute` sub-elements required by Alibaba Cloud:

- A mandatory `Attribute` element with the `Name` attribute set to `https://www.alibabacloud.com/SAML-Role/Attributes/Role`

This element contains one or more `AttributeValue` sub-elements that list the role can be assumed by the user in your IdP. The value of the `AttributeValue`

Role sub-element is a comma-delimited pair of role ARN and IdP ARN. You can obtain the role ARN and IdP ARN in the RAM console.

- To obtain the role ARN, go to the RAM Roles page and click the name of the target RAM role.
- To obtain the IdP ARN, go to the SSO page. On the Role-based SSO tab, click the name of the target IdP.

If the sub-element contains multiple pairs, the user is asked to select which role to assume during logon through the console.

The following is an example of the **Role** sub-element:

```
< Attribute Name = " https :// www . aliyun . com / SAML - Role /
Attributes / Role ">
  < AttributeV alue > acs : ram :: $ account_id : role / role1 , acs
: ram :: $ account_id : saml - provider / provider1 </ AttributeV
alue >
  < AttributeV alue > acs : ram :: $ account_id : role / role2 , acs
: ram :: $ account_id : saml - provider / provider1 </ AttributeV
alue >
</ Attribute >
```



Note:

The value of \$ **account_id** is the Alibaba Cloud account ID that defines the RAM role and IdP.

- A mandatory **Attribute** element with the **Name** attribute set to **https :// www . aliyun . com / SAML - Role / Attributes / RoleSessio nName**

This element contains only one **AttributeV alue** sub-element that is used to display user information in the RAM console and ActionTrail logs. If you want multiple users to assume one role, use a unique **RoleSessio nName** value, such as the user ID and email address for different users.

The value in the **AttributeV alue** sub-element must be 2 to 64 characters in length, and include only letters, digits, commas (,), periods (.), hyphens (-), underscores (_), plus signs (+), equal signs (=), and at signs (@).

The following is an example of the **RoleSessio nName** sub-element:

```
< Attribute Name = " https :// www . aliyun . com / SAML - Role /
Attributes / RoleSessio nName ">
  < AttributeV alue > user_id </ AttributeV alue >
```

```
</ Attribute >
```

- Optional, an `Attribute` element with the `Name` attribute set to `https://www.aliyuncs.com/SAML-Role/Attributes/SessionDuration`

This element contains only one `AttributeValue` sub-element that specifies the logon duration. If the logon is initiated through the console, the `AttributeValue` sub-element represents the number of seconds for the session. If the logon is initiated through the program, the `AttributeValue` sub-element represents the STS token validity.

The value of `AttributeValue` is an integer representing the logon duration, in seconds. The value can range from 900 seconds (15 minutes) to 3600 seconds (1 hour). If this sub-element does not exist, the logon duration is one hour.

The following is an example of the `SessionDuration` sub-element:

```
< Attribute Name = " https://www.aliyun.com/SAML-Role/Attributes/SessionDuration ">
  < AttributeValue > 1800 </ AttributeValue >
</ Attribute >
```

3.4.5 Implement role-based SSO by using AD FS

This topic provides an example of how to implement role-based Single Sign On (SSO) from AD FS to Alibaba Cloud, detailing the end-to-end identity SSO process from an enterprise identity provider (IdP) to Alibaba Cloud.

Scenario

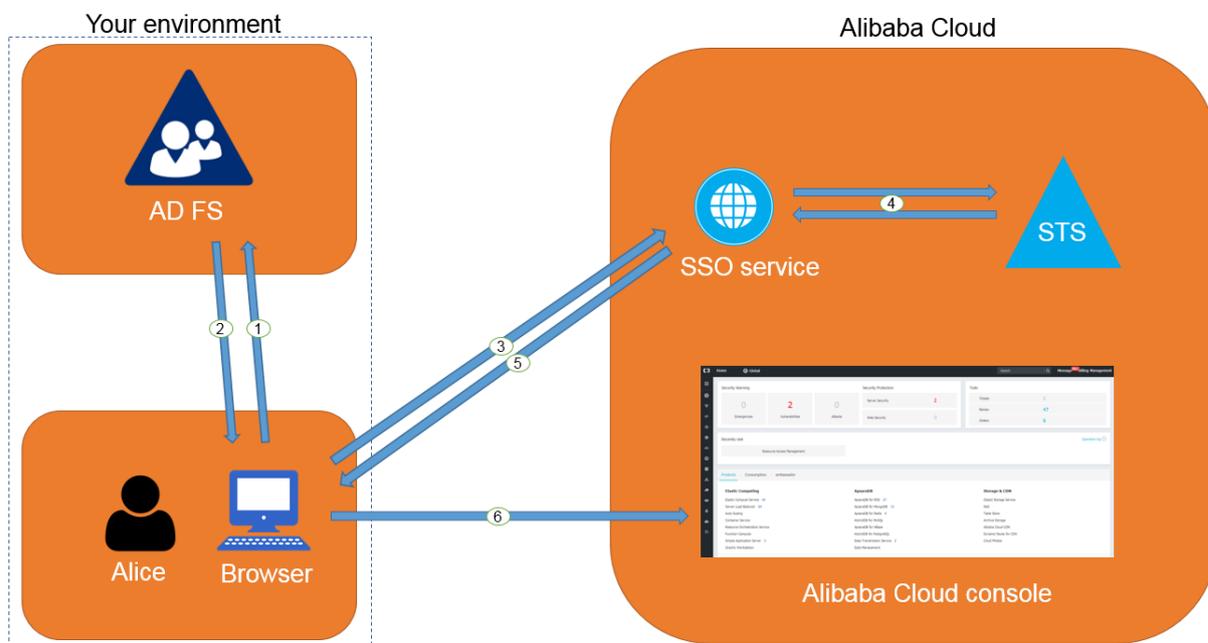
You use Active Directory (AD) to manage your users and use AD FS to configure enterprise applications such as Alibaba Cloud. Your AD administrator manages the access permissions on Alibaba Cloud accounts according to users' AD groups. In this example, you have two Alibaba Cloud accounts (Account1 and Account2), and the permissions managed by your AD administrator are Admin and Reader. You have a user named Alice. The AD groups of Alice are Aliyun-`<account-id>`-ADFS-Admin and Aliyun-`<account-id>`-ADFS-Reader. You want to implement SSO from AD FS to Account1 and Account2.



Note:

In the preceding groups, <account-id> is the account ID of Account1 or Account2. Therefore, Alice belongs to four AD groups, which correspond to the Admin and Reader permissions respectively.

The following figure shows the basic SSO process through the console.



After the AD administrator has completed role-based SSO configurations, Alice can log on to the Alibaba Cloud console by following the steps in the preceding figure. For more information, see [Role-based SSO overview](#).

The preceding SSO process shows that users of an enterprise can be authenticated with no need to provide Alibaba Cloud usernames and passwords during logon.

Configurations

To implement role-based SSO, the administrator must configure Alibaba Cloud and AD FS by following these steps:

- Configure AD FS as a trusted SAML IdP in Alibaba Cloud:
 1. Create an IdP named `ADFS` under Account1 in the Alibaba Cloud RAM console, and configure the corresponding metadata file. The metadata file of your AD FS can be obtained from `https ://< AD FS - server >/ federation metadata / 2007 - 06 / federation metadata . xml`.



Note:

In the preceding URL, <ADFS-server> is the server domain name or IP address of your AD FS.

For more information, see [Configure the SAML for role-based SSO](#).

2. Create two RAM roles named ADFS-Admin and ADFS-Reader under Account1, select `ADFS` you have created as the trusted entity, and attach the `AdministratorAccess` and `ReadOnlyAccess` policies to these two RAM roles respectively. For more information, see [RAM role management](#).
3. Create an IdP and two RAM roles under Account2 as described in the preceding steps, and attach policies to these two RAM roles.



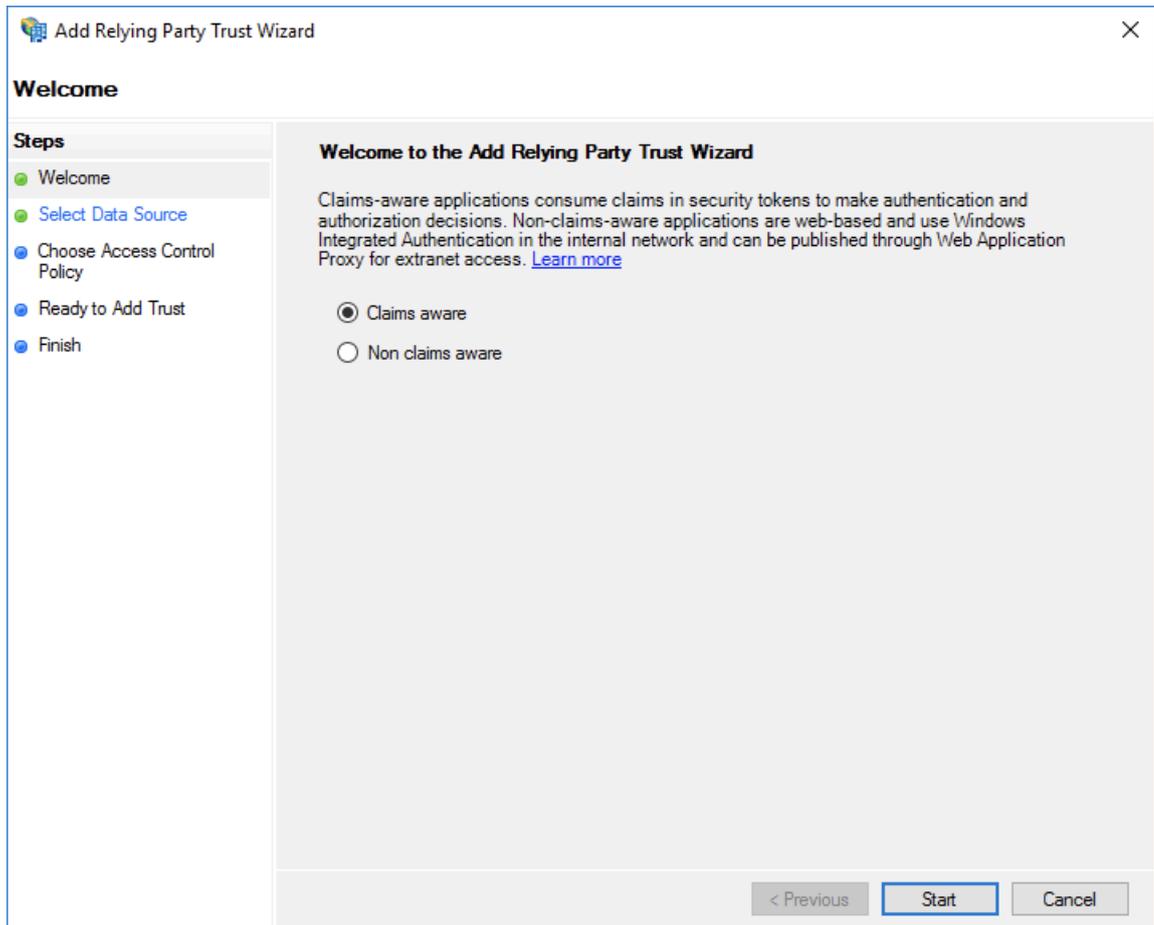
Note:

After the configurations are completed, your Alibaba Cloud accounts (Account1 and Account2) will trust the user identity and role information in the SAML requests sent from your AD FS.

- Configure Alibaba Cloud as a trusted SAML SP in AD FS.

In AD FS, SAML SP is also known as a relying party. To set Alibaba Cloud as a trusted SAML SP in AD FS, follow these steps:

1. On the Server Manager page, choose Tools > AD FS Management.
2. Select Add Relying Party Trust.



3. Set the SAML SP metadata of Alibaba Cloud for the relying party. The metadata URL is `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome (selected), Select Data Source (current), Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options:

- Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app
- Import data about the relying party from a file. Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location:
- Enter data about the relying party manually. Use this option to manually input the necessary data about this relying party organization.

At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted in blue), and 'Cancel'.

4. Complete the configurations as prompted.

- Configure the SAML assertion attributes for the Alibaba Cloud SP.

The SAML assertion issued by your AD FS must contain the attributes such as `NameID` , `Role` , and `RoleSessionName` . Your AD FS can provide these attributes by issuing transform rules.

- `NameID`

Follow these steps to configure the Windows account name of AD to be the `NameID` in the SAML assertion:

1. Right-click the display name of the relying party and select Edit Claim Rules.
2. Click Issuance Transform Rules.

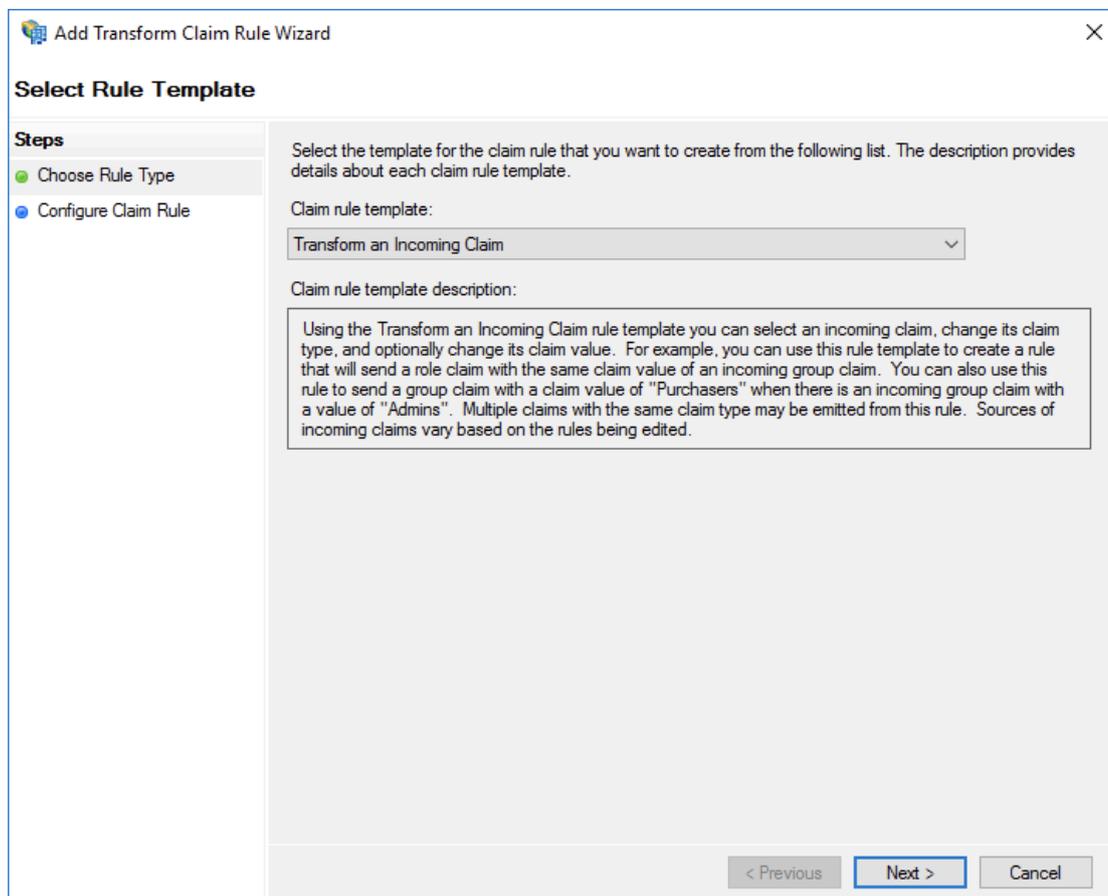


Note:

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

Windows account name of a user in AD as a `NameID` . This means that a new rule is required.

3. Select Transform an Incoming Claim from the Claim rule template drop-down list.



4. Configure the claim rule as follows, and click Finish.

- Claim rule name: NameID
- Incoming claim type: Windows account name
- Outgoing claim type: Name ID
- Outgoing name ID format: Persistent Identifier
- Pass through all claim values: Selected

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

Pass through all claim values
 Replace an incoming claim value with a different outgoing claim value
 Incoming claim value:
 Outgoing claim value:
 Replace incoming e-mail suffix claims with a new e-mail suffix
 New e-mail suffix:
 Example: fabrikam.com

After the configurations are completed, AD FS will send the required `NameID` format to Alibaba Cloud. The following is an example:

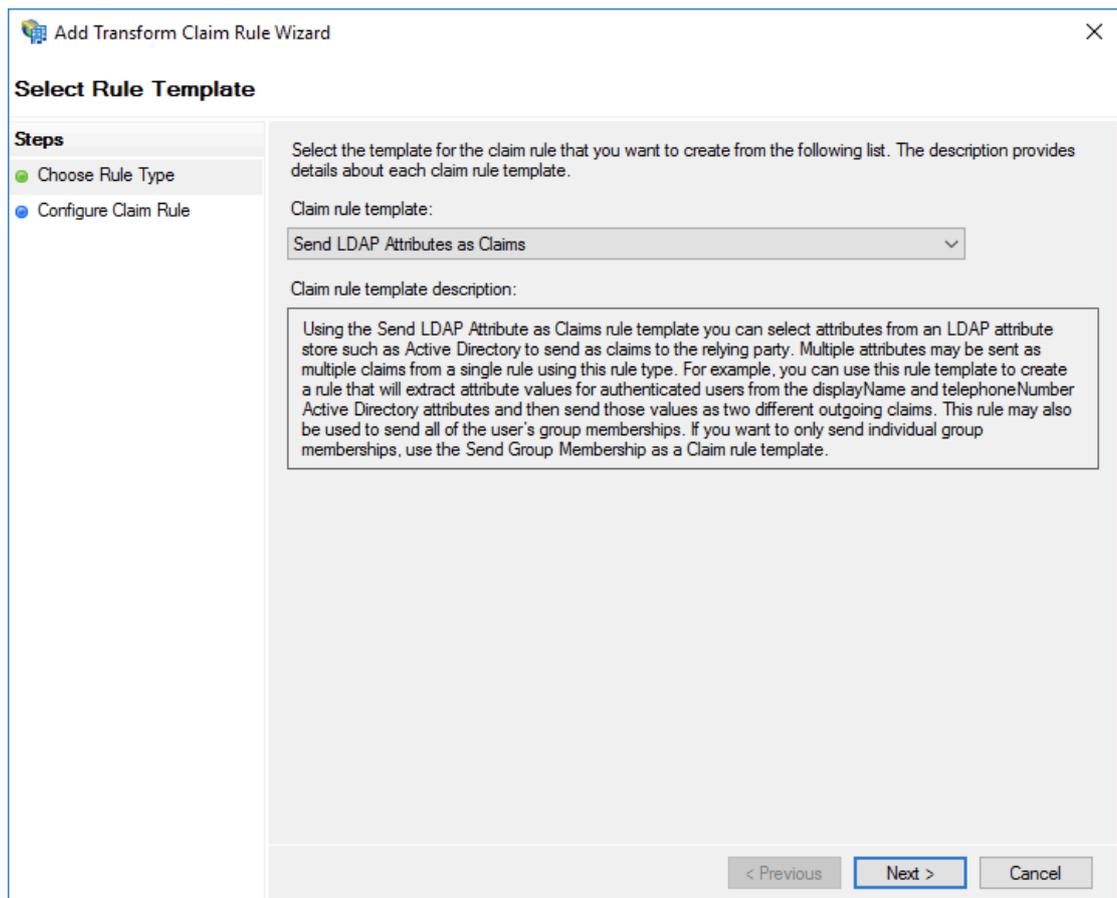
```
< NameID Format = " urn : oasis : names : tc : SAML : 2 . 0 :
nameid - format : persistent ">
YourDomain \ rolessouse r
```

```
</ NameID >
```

- RoleSessionName

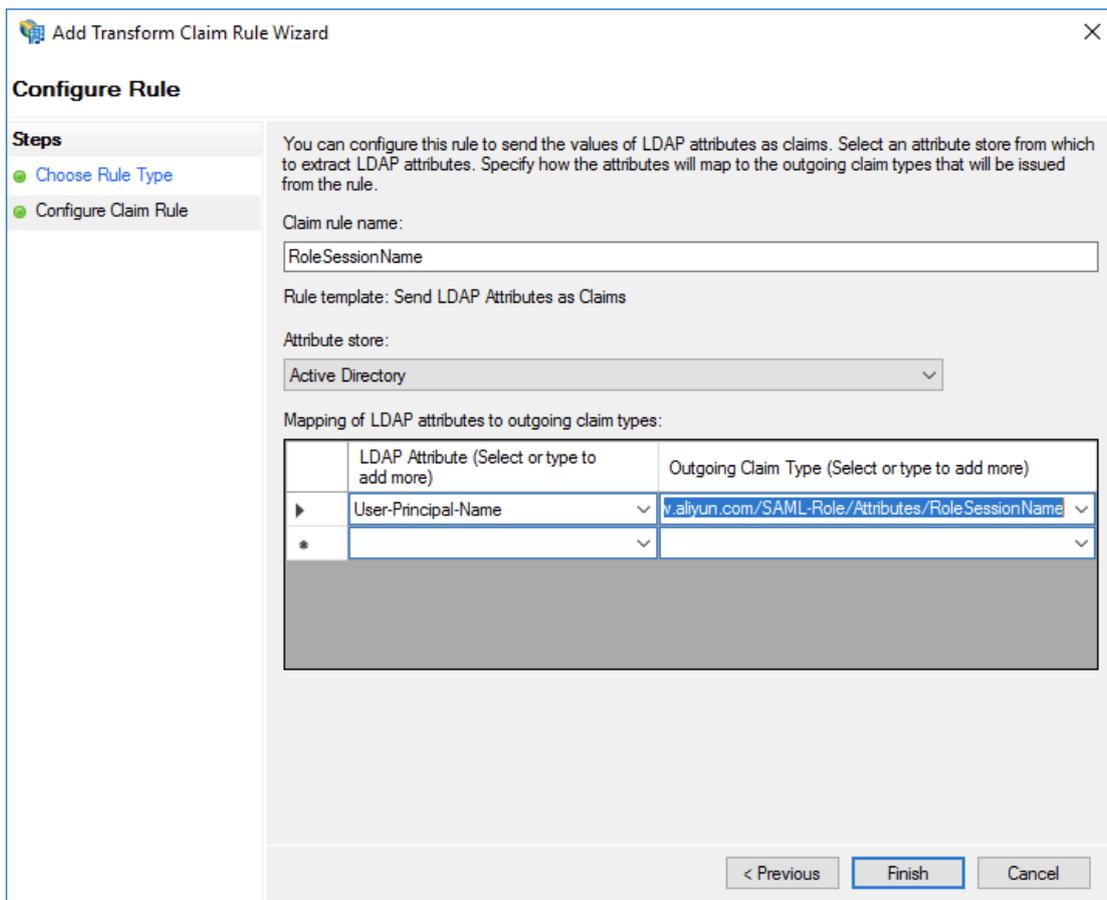
Follow these steps to configure the UPN of AD to the RoleSessionName in the SAML assertion:

1. Click Add Transform Claim Rule.
2. Select Send LDAP Attributes as Claims from the Claim rule template drop-down list.



3. Configure the claim rule as follows, and click Finish.

- Claim rule name: RoleSessionName
- Attribute store: Active Directory
- LDAP Attribute: User-Principal-Name (You can select other attributes, such as Email, as needed.)
- Outgoing Claim Type: https://www.aliyun.com/SAML-RoleSessionName/Attributes/RoleSessionName



After the configurations are completed, AD FS will send the required RoleSessionName format to Alibaba Cloud. The following is an example:

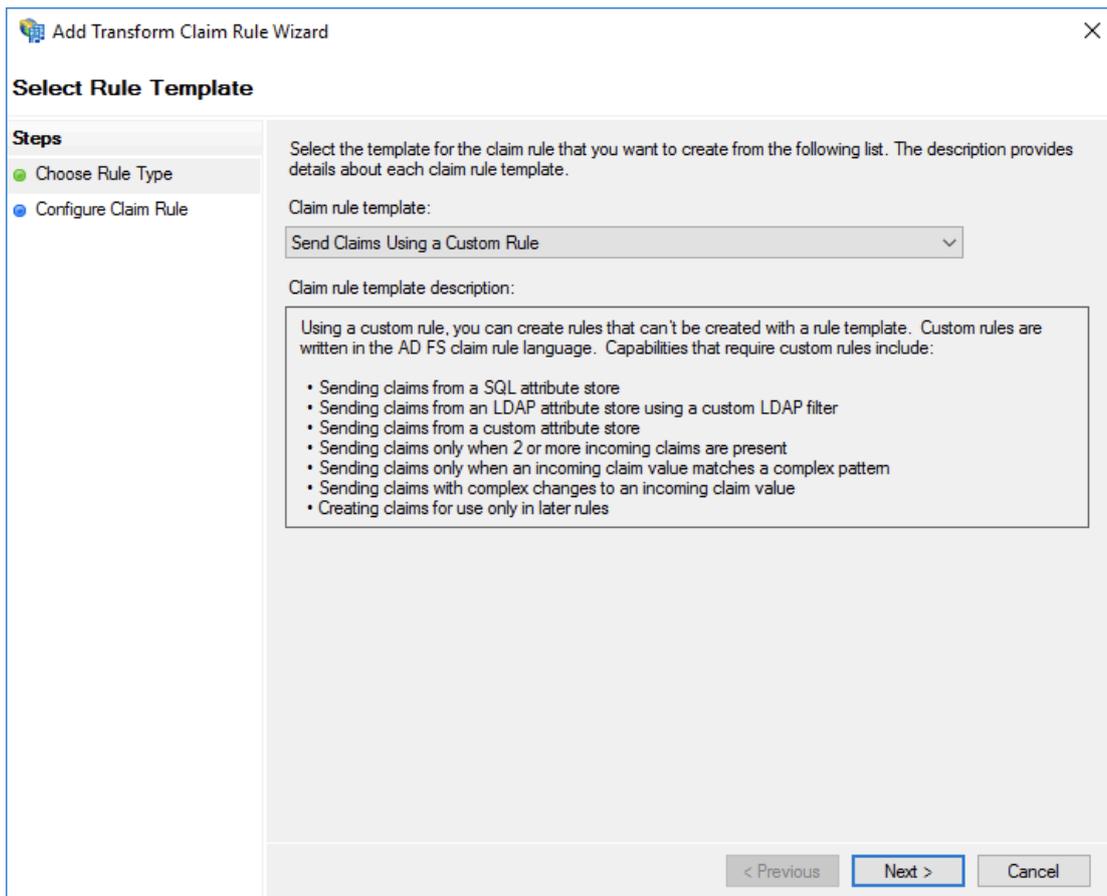
```
< Attribute Name = " https :// www . aliyun . com / SAML - Role /
Attributes / RoleSessio nName ">
  < AttributeV alue > rolessouse r @ example . com <
AttributeV alue >
```

```
</ Attribute >
```

- Role

Follow these steps to transform the user's AD group membership into the role name of Alibaba Cloud by using custom rules:

1. Click Add Transform Claim Rule.
2. Select Send Claims Using a Custom Rule from the Claim rule template drop-down list and click Next.

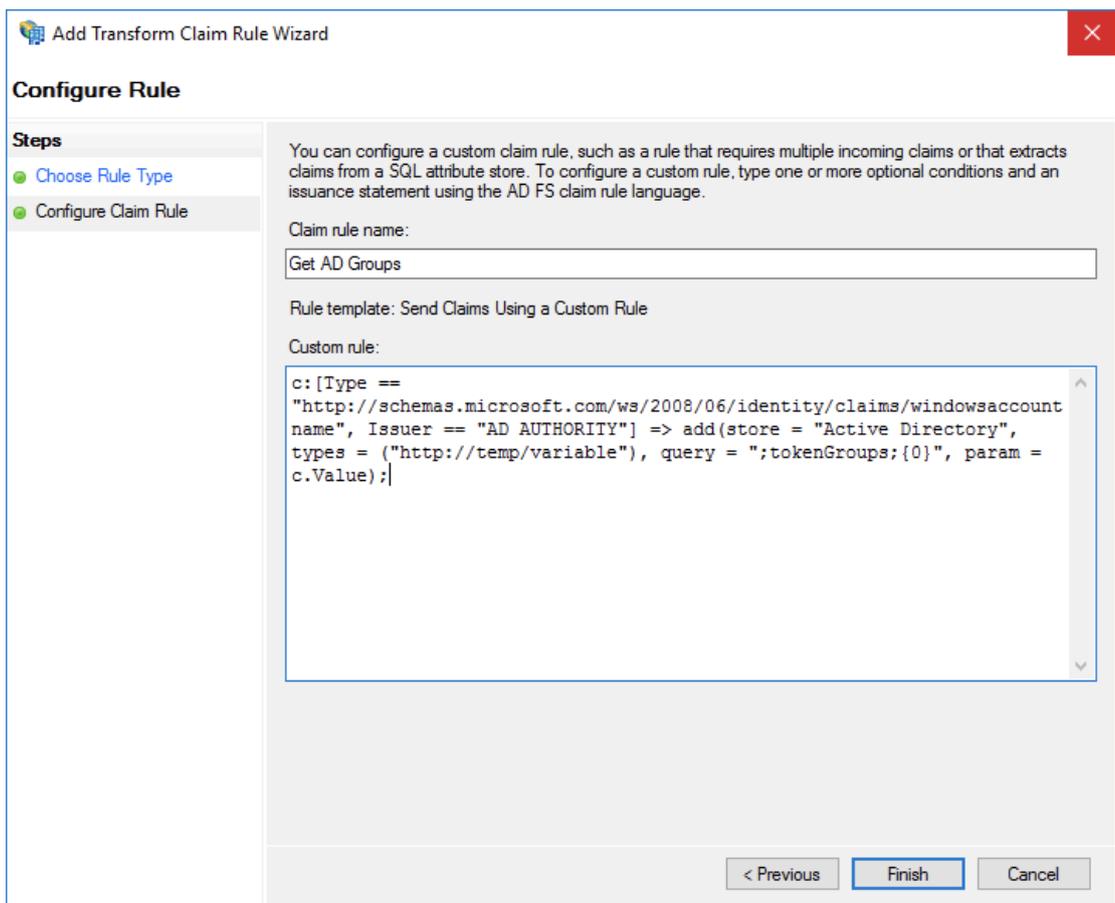


3. Configure the claim rule as follows, and click Finish.

- Claim rule name: Get AD Groups
- Custom rule:

```
c :[ Type ==
" http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY "] => add ( store = "Active Directory",
types = (" http://temp/variable"), query = ";tokenGroups;{0}"; param =
```

```
c . Value );
```



Note:

This rule is used to obtain the user's AD group membership and save it to *http://temp/variable*.

4. Click Add Transform Claim Rule.
5. Repeat the preceding steps and click Finish.

■ **Claim rule name:** Role

■ **Custom rule:**

```
c :[ Type == " http :// temp / variable ", Value =~ "(? i )^ Aliyun -([\ d ]+)" ] => issue ( Type = " https :// www . aliyun . com / SAML - Role / Attributes / Role ", Value = RegExRepla ce ( c . Value , " Aliyun -([\ d ]+)- (.+)", " acs : ram ::
```

```
$ 1 : role /$ 2 , acs : ram ::$ 1 : saml - provider / ADFS
")));
```

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:
Role

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^Aliyun-([\d]+)"]
=> issue(Type = "https://www.aliyun.com/SAML-Role/Attributes/Role",
Value = RegExReplace(c.Value, "Aliyun-([\d]+)-(.+)", "acs:ram::
$1:role/$2,acs:ram::$1:saml-provider/ADFS"));
```

< Previous Finish Cancel



Note:

According to this rule, if the user's AD group contains Aliyun-**<account-id>**-ADFS-Admin or Aliyun-**<account-id>**-ADFS-Reader, an SAML attribute will be generated and sent to Alibaba Cloud to match the RAM role ADFS-Admin or ADFS-Reader.

After the configurations are completed, your IdP will return a required SAML assertion to Alibaba Cloud. The following is an example:

```
< Attribute Name = " https :// www . aliyun . com / SAML - Role /
Attributes / Role ">
  < AttributeV alue > acs : ram ::< account - id >: role / ADFS
- Admin , acs : ram ::< account - id >: saml - provider / ADFS </
AttributeV alue >
```

```
</ Attribute >
```

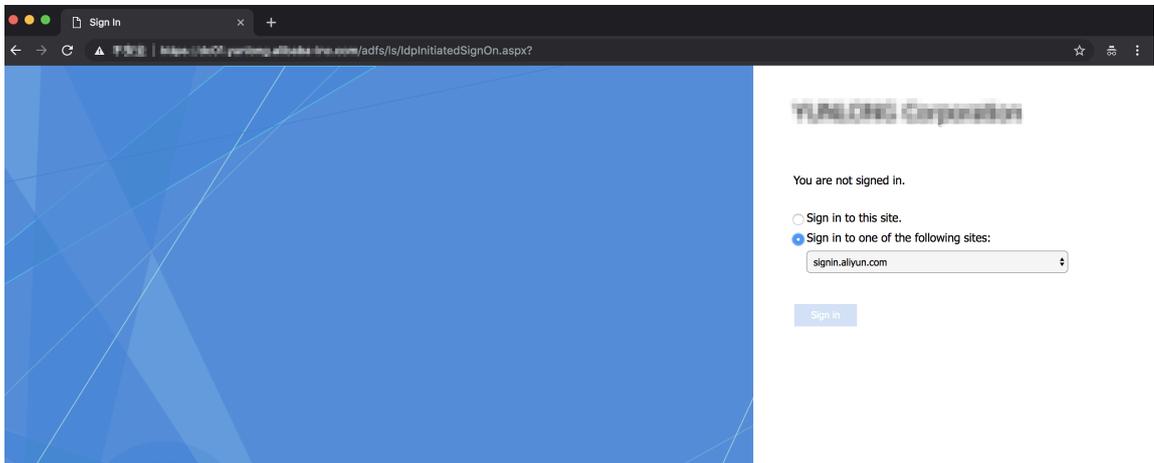
Verification

1. Log on to the AD FS SSO portal (URL: `https://< ADFS - server >/ adfs / ls / IdpInitiat edSignOn . aspx`), select Alibaba Cloud application, and enter the username and password.



Note:

In the preceding URL, <ADFS-server> is the server domain name or IP address of your AD FS. If the URL does not work, run the PowerShell `Set - AdfsProper ties - EnableIdpI nitiatedSi gnonPage $ True` .

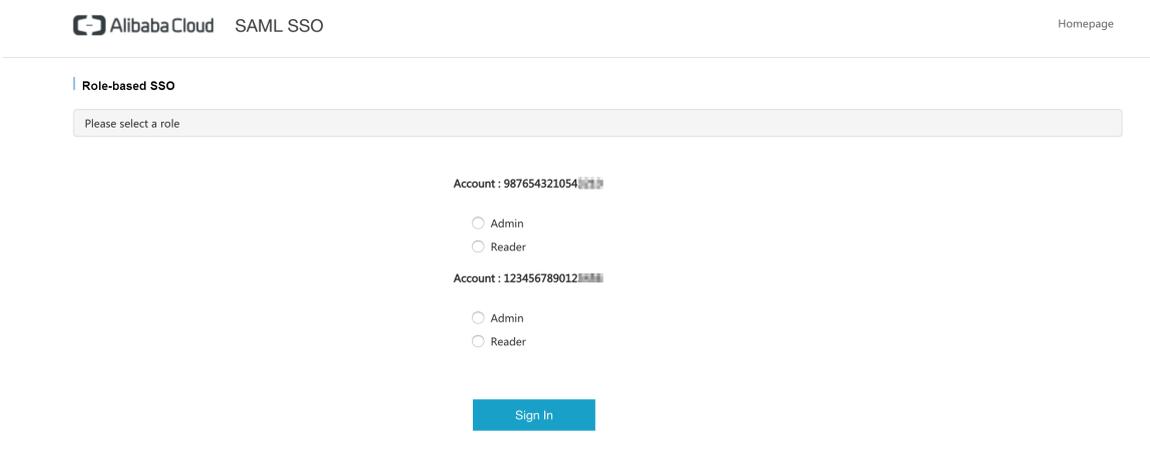


2. On the Alibaba Cloud role-based SSO page, select the target role and click Sign In.



Note:

If your user belongs to only one AD group, the user can log on to Alibaba Cloud with no need of selecting a role.



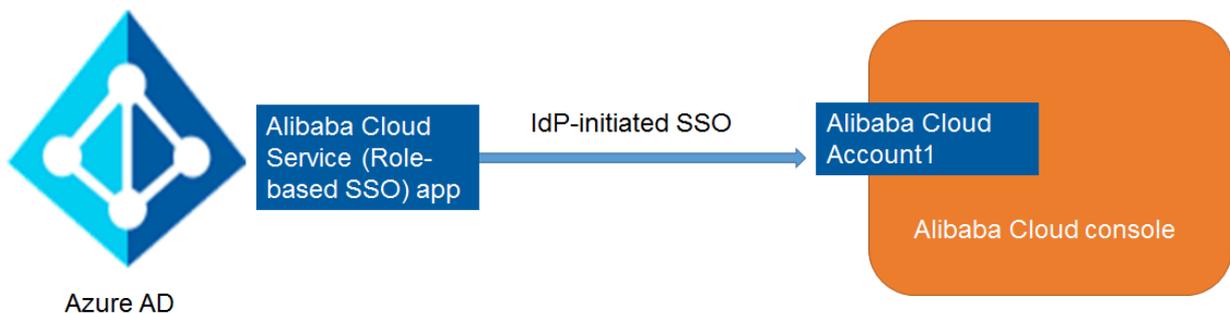
3.4.6 Implement role-based SSO by using Azure Active Directory

This topic provides an example of how to implement role-based Single Sign On (SSO) to Alibaba Cloud from Azure Active Directory (Azure AD), detailing the end-to-end identity SSO process from a cloud identity provider (IdP) to Alibaba Cloud. After implementing role-based SSO, you can better manage your Azure AD users who have access to Alibaba Cloud, enable your users to automatically log on to Alibaba Cloud with their Azure AD accounts, and manage your accounts in the Azure portal.

Scenario

You use Azure AD to manage your users and configure enterprise applications such as Alibaba Cloud. In this example, you have an Alibaba Cloud account (Account1) and a user named u2. You want u2 to implement SSO from Azure AD to Account1.

The following figure shows the basic SSO process.



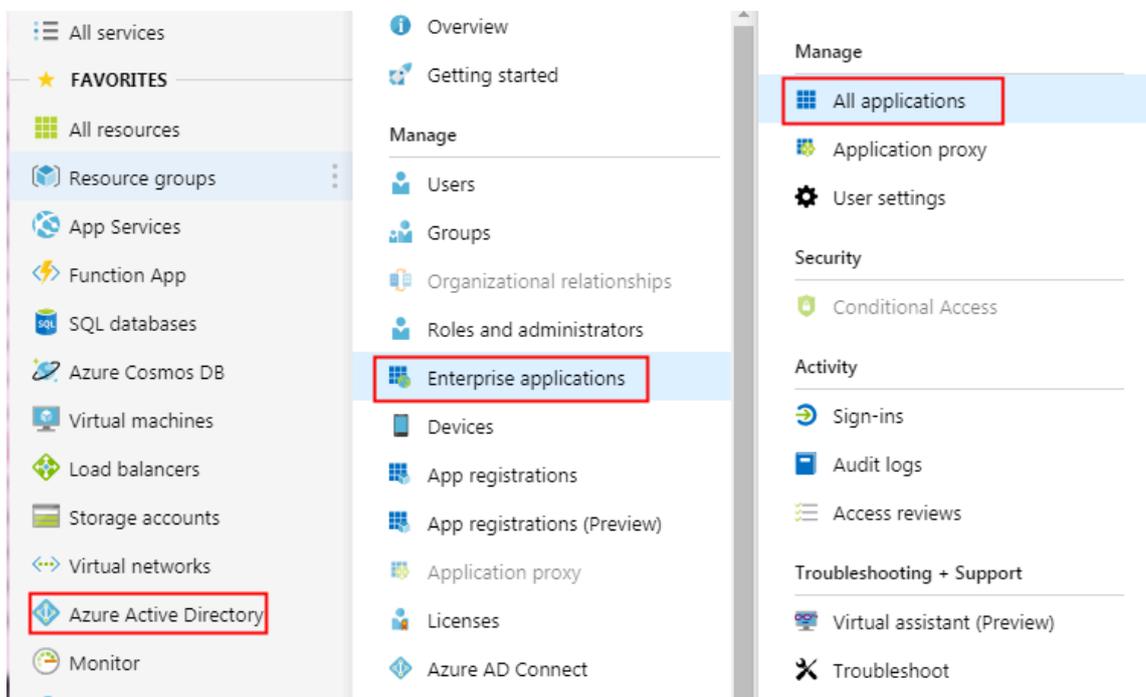
 **Note:**

You can also implement role-based SSO from Azure AD to multiple Alibaba Cloud accounts by connecting multiple Alibaba Cloud (Role-based SSO) apps.

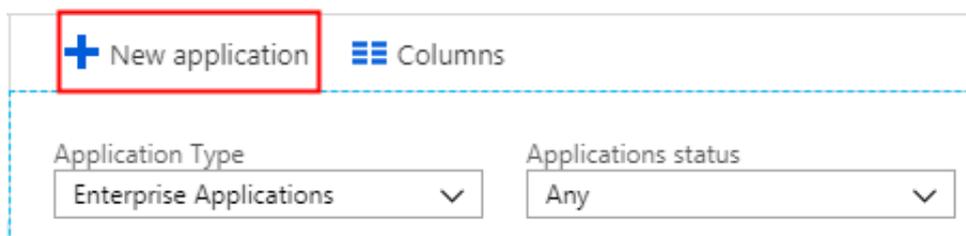
Configurations

To implement role-based SSO, you must configure Azure AD and Alibaba Cloud by following these steps:

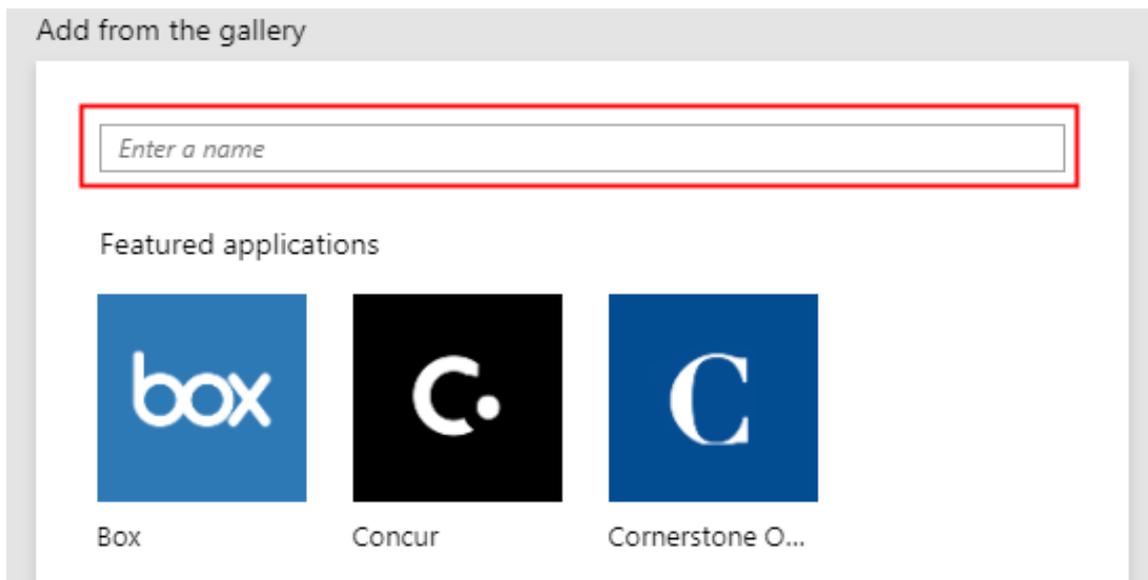
- Add Alibaba Cloud role-based SSO from Azure AD gallery:
 1. Log on to the [Azure portal](#).
 2. In the left-side navigation pane, choose Azure Active Directory > Enterprise applications > All applications.



3. Click New application.



4. On the displayed page, enter Alibaba Cloud Service (Role-based SSO) in the search box, press Enter, and select Alibaba Cloud Service (Role-based SSO).



5. On the displayed page, click Add.

Name ⓘ
Alibaba Cloud Service (Role-based SSO)

Publisher ⓘ
Alibaba Group

Single Sign-On Mode ⓘ
SAML-based sign-on

URL ⓘ
<https://www.aliyun.com>

Logo ⓘ



[Read our step-by-step Alibaba Cloud Service \(Role-based SSO\) integration tutorial](#)

Add

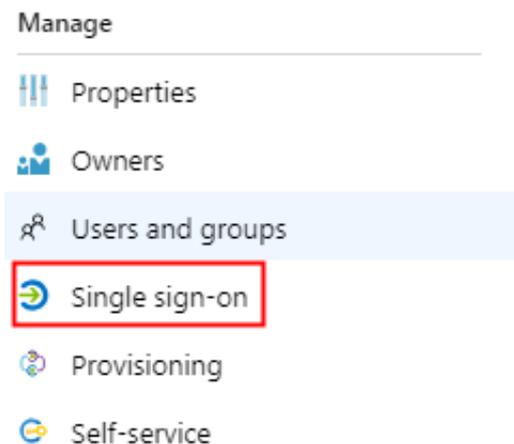
6. On the Alibaba Cloud Service (Role-based SSO) page, click Properties in the left-side navigation pane, and copy and save the object ID for subsequent use.

The screenshot displays the 'Properties' configuration page for an application named 'Alibaba Cloud Service (Role-based SSO)'. The left sidebar contains navigation options: Overview, Getting started, Deployment Plan, Manage (Properties, Owners, Users and groups, Single sign-on, Provisioning, Self-service), Security (Conditional Access, Permissions, Token encryption (Preview)), Activity (Sign-ins, Audit logs), and Troubleshooting + Support (Virtual assistant (Preview), Troubleshoot, New support request). The main configuration area includes the following fields:

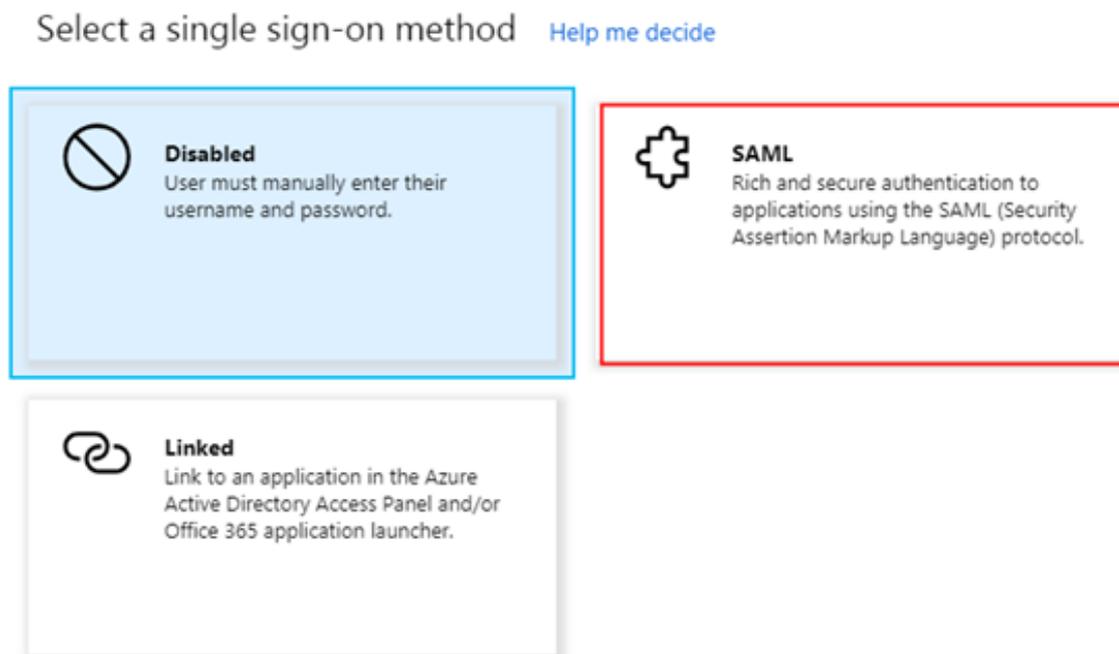
- Name: Alibaba Cloud Service (Role-based SSO)
- Homepage URL: https://www.aliyun.com
- Logo: A placeholder image of a square with a minus sign.
- User access URL: A redacted field with a copy icon.
- Application ID: A redacted field with a copy icon.
- Object ID: A redacted field with a copy icon, highlighted by a red box.
- Terms of Service URL: A redacted field with a copy icon.
- Privacy Statement URL: A redacted field with a copy icon.
- Reply URL: A redacted field with a copy icon.
- User assignment required?: A toggle switch set to 'Yes'.
- Visible to users?: A toggle switch set to 'Yes'.

• Enable Azure AD SSO in Azure AD:

1. In the Azure portal, choose Azure Active Directory > Enterprise applications > All applications.
2. In the NAME column, click Alibaba Cloud Service (Role-based SSO).
3. On the displayed page, select Single sign-on from the left-side navigation pane.



4. In the Select a single sign-on method section, click SAML.



5. On the Set up Single Sign-On with SAML page, follow these steps:

- a. In the upper-left corner, click Upload metadata file to integrate Azure AD with Alibaba Cloud role-based SSO, and click Save.





Note:

You can obtain the metadata file from the URL `https://signin.alibabaclo ud . com / saml - role / sp - metadata . xml .`

b. In the User Attributes & Claims section, click the Edit icon.



c. Click Add new claim. In the Name field, enter `Role` . In the Namespace field, enter `https://www.aliyun.com/SAML-Role/Attribute` . Set Source to Attribute, select `user.assignedroles` from the Source attribute drop-down list, and click Save.

* Name	<input type="text" value="Role"/>
Namespace	<input type="text" value="https://www.aliyun.com/SAML-Role/Attribute"/>
Source	<input checked="" type="radio"/> Attribute <input type="radio"/> Transformation
* Source attribute	<input type="text" value="user.assignedroles"/>

d. Repeat the preceding step to add a new claim with Name set to `RoleSessionName` and Source attribute set to `user.userprincipalname` , and click Save.



Note:

You can also enter `https://www.aliyun.com/SAML-Role/Attribute` in the Namespace field.

- e. In the SAML Signing Certificate section, click Download to download the federation metadata XML for subsequent use.

3

SAML Signing Certificate	
Status	Active
Thumbprint	D0AA0885D8EC8CC9FC24AD03C8DB08CF2B3C848D
Expiration	4/9/2022, 9:33:27 AM
Notification Email	1406281081@qq.com
App Federation Metadata Url	https://login.microsoftonline.com/878f14...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- f. In the Set up Alibaba Cloud Service (Role-based SSO) section, copy the URLs as needed.

4

Set up Alibaba Cloud Service (Role-based SSO)

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/878f14...
Azure AD Identifier	https://sts.windows.net/878f1420-238a-4...
Logout URL	https://login.microsoftonline.com/commo...

[View step-by-step instructions](#)

• Configure role-based SSO in Alibaba Cloud:

1. Log on to the Alibaba Cloud [RAM console](#) by using Account1.
2. In the left-side navigation pane, select SSO.
3. On the Role-based SSO tab, click Create IdP.
4. On the displayed page, enter `AAD` in the IdP Name field, enter a description in the Note field, click Upload to upload the federation metadata file you downloaded before, and click OK.
5. After the IdP is successfully created, click Create RAM Role.
6. In the RAM Role Name field, enter `AADrole`, select `AAD` from the Select IdP drop-down list, and click OK.



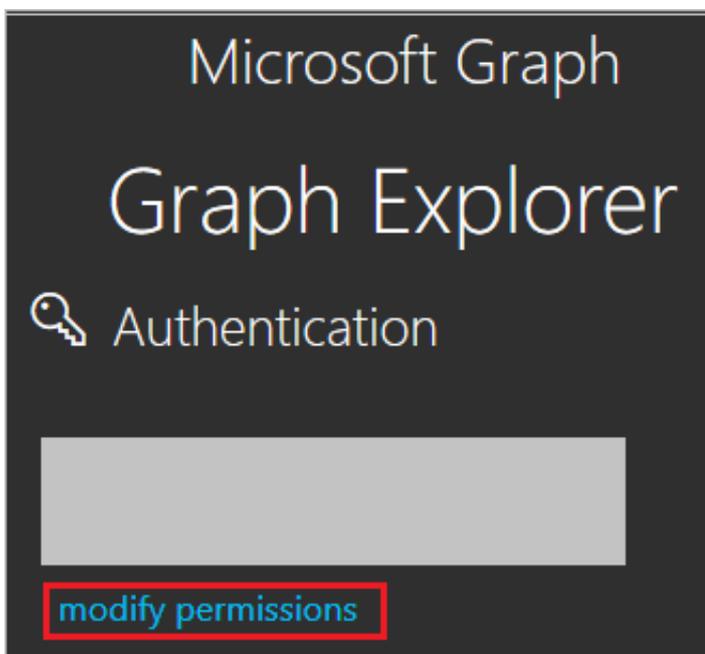
Note:

You can grant permission to the role as needed. After creating the IdP and the corresponding role, we recommend that you save the ARNs of the IdP and the role for subsequent use. You can obtain the ARNs on the IdP information page and the role information page.

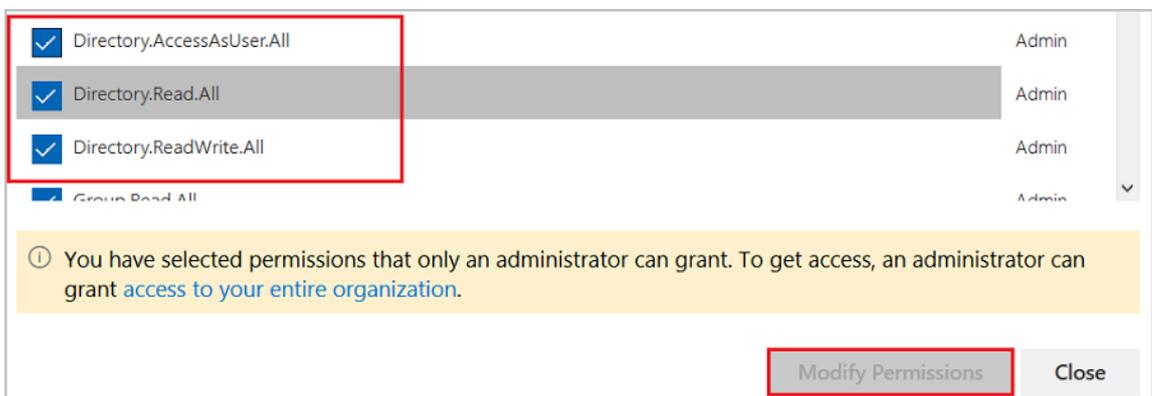
- Associate the Alibaba Cloud RAM role (AADrole) with the Azure AD user (u2):

To associate the RAM role with the Azure AD user, you must create a role in Azure AD by following these steps:

1. Log on to the [Azure AD Graph Explorer](#).
2. Click modify permissions to obtain required permissions for creating a role.



3. Select the following permissions from the list and click Modify Permissions, as shown in the following figure.



 **Note:**

After permissions are granted, log on to the Graph Explorer again.

4. On the Graph Explorer page, select GET from the first drop-down list and beta from the second drop-down list. Then enter `https://graph.microsoft.com/beta/servicePrincipals` in the field next to the drop-down lists, and click Run Query.

Request Body Request Headers

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#servicePrincipals",
  "@odata.nextLink": "https://graph.microsoft.com/beta/servicePrincipals?$skiptoken=...",
  "value": [
    {
      "id": "...",
      "deletedDateTime": null,
      "accountEnabled": true,
      "appDisplayName": "Substrate Instant Revocation Pipeline",
      "appId": "..."
    }
  ]
}
```

 **Note:**

If you are using multiple directories, you can enter `https://graph.microsoft.com/beta/contoso.com/servicePrincipals` in the field of the query.

5. In the Response Preview section, extract the `appRoles` property from the 'Service Principal' for subsequent use.

```

"appRoles": [
  {
    "allowedMemberTypes": [
      "User"
    ],
    "description": "msiam_access",
    "displayName": "msiam_access",
    "id": "XXXXXXXXXXXXXXXXXXXX",
    "isEnabled": true,
    "origin": "Application",
    "value": null
  }
],

```



Note:

You can locate the `appRoles` property by entering `https://graph.microsoft.com/beta/servicePrincipals/<objectID>` in the field of the query. Note that the `objectID` is the object ID you have copied from the Azure AD Properties page.

6. Go back to the Graph Explorer, change the method from GET to PATCH, paste the following content into the Request Body section, and click Run Query:

```

{
  " appRoles ": [
    {
      " allowedMem berTypes ":[
        " User "
      ],
      " descriptio n ": " msiam_acce ss ",
      " displayNam e ": " msiam_acce ss ",
      " id ": " 41be2db8 - 48d9 - 4277 - 8e86 - f6d22d35 ****",
      " isEnabled ": true ,
      " origin ": " Applicatio n ",
      " value ": null
    },
    { " allowedMem berTypes ": [
      " User "
    ],
      " descriptio n ": " Admin , AzureADPro d ",
      " displayNam e ": " Admin , AzureADPro d ",
      " id ": " 68adae10 - 8b6b - 47e6 - 9142 - 6476078cdb ce ",

```

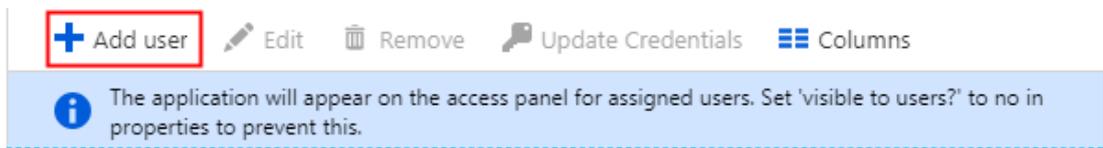
```
" isEnabled ": true ,
" origin ": " ServicePrincipal ",
" value ": " acs : ram :: 1871250227 22 ****: role / aadrole
, acs : ram :: 1871250227 22 ****: saml - provider / AAD "
}
]
}
```

**Note:**

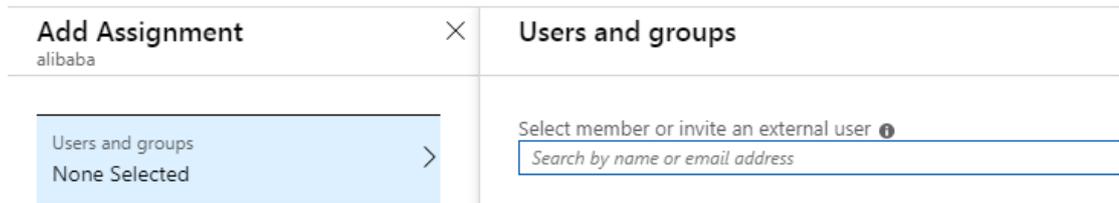
The `value` is the ARNs of the IdP and the role you created in the RAM console. Here, you can add multiple roles as needed. Azure AD will send the value of these roles as the claim value in SAML response. However, you can only add new roles after the `msiam_access` part for the patch operation. To

smooth the creation process, we recommend that you use an ID generator, such as GUID Generator, to generate IDs in real time.

7. After the 'Service Principal' is patched with the required role, attach the role with the Azure AD user (u2) by following these steps:
 - a. In the Azure portal, choose Azure Active Directory > Enterprise applications > All applications.
 - b. In the NAME column, click Alibaba Cloud Service (Role-based SSO).
 - c. On the displayed page, select Users and groups from the left-side navigation pane.
 - d. In the upper-left corner, click Add user.



- e. On the Users and groups tab, select u2 from the user list, and click Select. Then, click Assign.



- f. View the assigned role and test role-based SSO.

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
 u2	User	Admin, AzureADProd



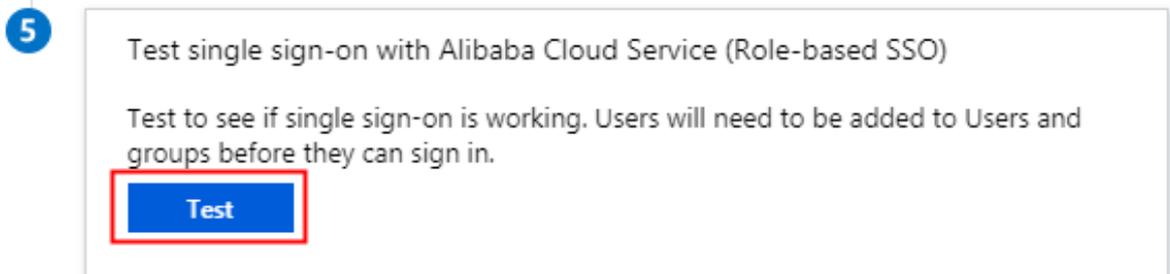
Note:

After you assign the user (u2), the created role is automatically attached to the user. If you have created multiple roles, you need to attach the appropriate role to the user as needed. If you want to implement role-based SSO from Azure AD to multiple Alibaba Cloud accounts, repeat the preceding steps.

Test role-based SSO

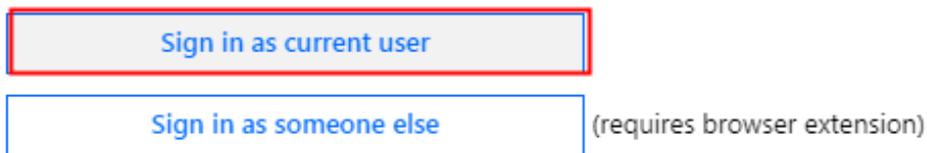
After the preceding configurations are completed, test role-based SSO by following these steps:

1. In the Azure portal, go to the Alibaba Cloud Service (Role-based SSO) page, select Single sign-on, and click Test.

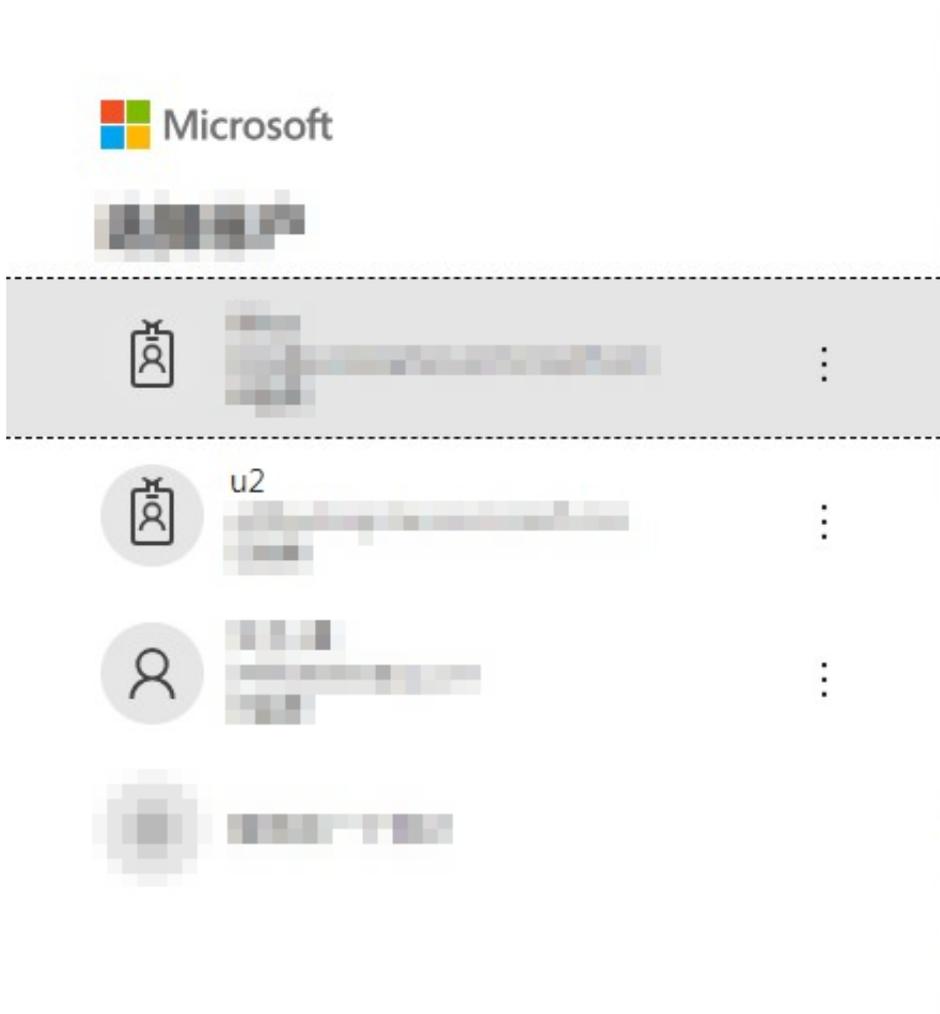


2. Click Sign in as current user.

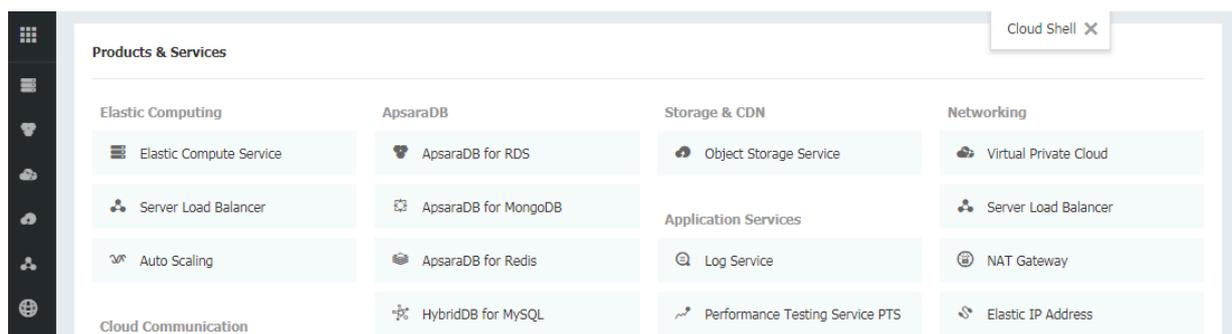
Please make sure you have configured Alibaba Cloud Service (Role-based SSO) before testing.



3. On the account selection page, select u2.



The following page is displayed, indicating that role-based SSO is successful.



4 Permission management

4.1 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 structure and 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.

4.2 Policy management

This topic describes how to manage different types of policies. Types of policies include system policies and custom policies. System policies can be viewed but cannot be modified, whereas custom policies can be created to meet your needs as required.

Before creating a custom policy

Before you create a custom policy, we recommend that you read about the basic structure and syntax of a policy. For more information, see [Policy structure and syntax](#).

Create a custom policy

1. Log on to the [RAM console](#).
2. Choose Permissions > Policies.
3. Click Create Policy.
4. Enter a name for the Policy Name. You can also enter a description in Note.
5. Set Configuration Mode to Visualized or Script.
 - If you set the configuration mode to Visualized, click Add Statement and configure the permission effect, actions, and resources as prompted.
 - If you set the configuration mode to Script, edit the policy according to [Policy structure and syntax](#).

Modify a custom policy

Scenario

If the permissions of a user are changed (added or removed), you must modify the corresponding policy associated to the user. However, 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.

Procedure

1. In the RAM console, choose Permissions > Policies.
2. In the Policy Name column, click the target policy name.



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, that is, the default version. If multiple versions exist, you can 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, select the target policy and click Delete on the right.



Note:

You can enter keywords to search for a specific policy.

3. In the Delete Custom Policy dialog box, click OK.

4.3 Permission granting

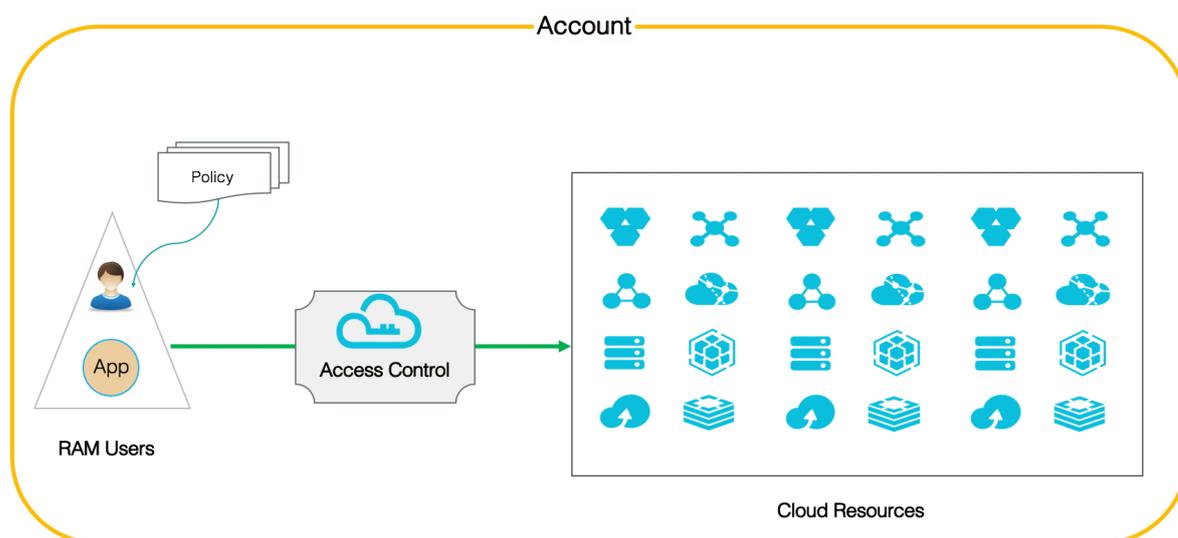
4.3.1 Permission model overview

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 4-1: Model of granting permissions for an account



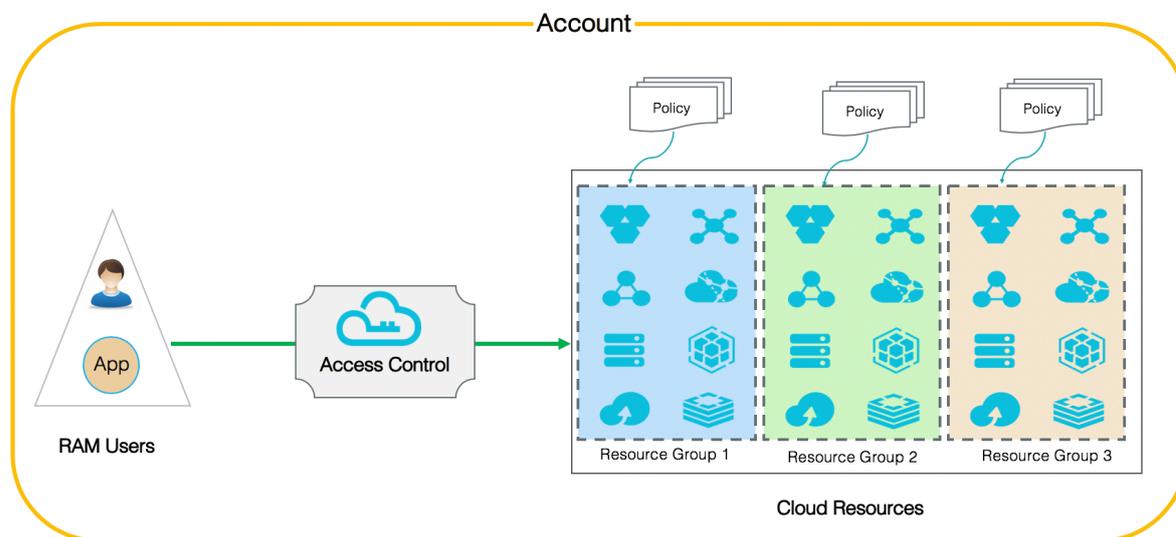
Grant permissions for one or more target resource groups

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 4-2: Model of granting permissions for a resource group



4.3.2 Permission granting in RAM

This topic describes how to attach one or more policies to RAM identities (that is, RAM users, RAM user groups, or RAM roles) under an Alibaba Cloud account.

Scenarios

- Granting permission to RAM users mainly refers to granting permission to users under your account, so that the users can access the necessary resources.
- Granting permission to RAM user groups mainly refers to granting permission to groups under your account. After you grant permission to a RAM user group, all users in the group share the same permissions.
- Granting permission to RAM roles mainly refers to granting permission to standalone operations and applications, 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.

Before granting permission in RAM

Log on to the [RAM console](#).

Grant permission to a RAM user

1. Log on to the RAM console and choose Identities > Users.
2. In the User Logon Name/Display Name column, select the target user and click Add Permissions.
3. In the Policy Name column on the left, select the target policies and click OK.

**Note:**

To remove a policy, select the policy from the area on the right, and then click ×.

Grant permission to a RAM user group

1. Log on to the RAM console and choose Identities > Groups.
2. In the Group Name/Display Name column, select the target group and click Add Permissions.
3. In the Policy Name column on the left, select the target policies and click OK.

**Note:**

To remove a policy, select the policy from the area on the right, and then click ×.

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), Alibaba Cloud Service, or IdP. You must enter the corresponding trusted account ID, select the trusted service, or select the trusted identity provider (IdP) as needed.

- If you select Alibaba Cloud Account and Current Alibaba Cloud Account, the RAM users under the current account can assume the RAM role (that is, be 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 (that is, be authorized to access the required cloud resources).
- If you select Alibaba Cloud Service, the trusted cloud services can assume the RAM role (that is, be authorized to access the required cloud resources).
- If you select IdP, the users in the trusted IdP can assume the RAM role (that is, be authorized to access the required cloud resources).

1. Log on to the RAM console and click RAM Roles.
2. In the Role Name column, select the target RAM role and click Add Permissions.

3. In the Policy Name column on the left, select the target policies and click OK.



Note:

To remove a policy, select the policy from the area on the right, and then click ×.

4.4 Policy language

4.4.1 Policy elements

This topic describes the elements of policies that are used in Alibaba Cloud RAM to define a permission.

Elements

The following table describes the policy elements.

Element	Description
Effect	Effect can be either Allow or Deny.
Action	Actions are operations performed on specific resources.
Resource	Resources are the objects being authorized.
Condition	Conditions are the circumstances under which a permission takes effect.

How to use a policy element

- Effect

The value can be either 'Allow' or 'Deny', for example, " Effect ": " Allow ".

- Action

Action can have multiple values. The values are API operations defined by the target cloud services.



Note:

Actions are operations performed on specific resources. In most cases, an action corresponds to an Alibaba Cloud API. For more information about the actions

supported by different Alibaba Cloud products, see [Alibaba Cloud services that work with RAM](#).

Format:

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

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

Example:

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

• Resource

Resource generally specifies the object of operations.

Format:

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

- `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, rds, slb, 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` . If no ID is required or available, 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.

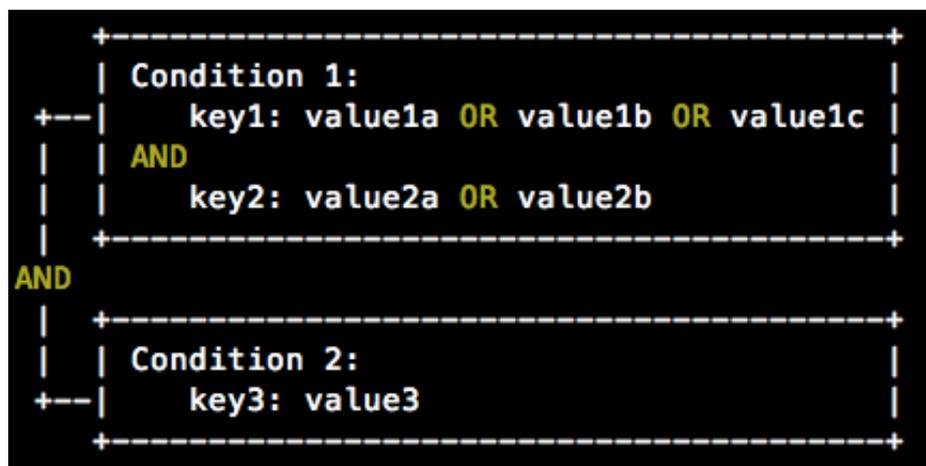
Example:

```
" 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.

Figure 4-3: 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.

Operation type	Supported type
String	<ul style="list-style-type: none"> - StringEquals - StringNotEquals - StringEqualsIgnoreCase - StringNotEqualsIgnoreCase - StringLike - StringNotLike

Operation type	Supported type
Numeric	<ul style="list-style-type: none"> - NumericEquals - NumericNotEquals - NumericLessThan - NumericLessThanEquals - NumericGreaterThan - NumericGreaterThanEquals
Date and time	<ul style="list-style-type: none"> - DateEquals - DateNotEquals - DateLessThan - DateLessThanEquals - DateGreaterThan - DateGreaterThanEquals
Boolean	Bool
IP address	<ul style="list-style-type: none"> - IpAddress - NotIpAddress

Condition keyword

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

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

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

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

Table 4-1: Common condition keywords

Common condition keyword	Type	Description
acs : CurrentTime	Date and time	Time when the Web server receives a request. This keyword is defined in ISO 8601 format, for example, 2012 - 11 - 11T23 : 59 : 59Z .

Common condition keyword	Type	Description
<code>acs : SecureTransport</code>	Boolean	Indicates whether a secure channel, such as HTTPS, is used to send a request.
<code>acs : SourceIp</code>	IP address	IP address of the client that sends a request.
<code>acs : MFAPresent</code>	Boolean	Indicates whether multi-factor authentication is used during user logon.

Table 4-2: Product-related condition keywords

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

Policy 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 :*:*: samplebuck et ", " acs :
oss :*:*: samplebuck et /*"],
    " Condition ":
    {
      " IPAddress ":
      {
        " acs : SourceIp ": " 42 . 160 . 1 . 0 "
      }
    }
  }
}

```

4.4.2 Policy structure and syntax

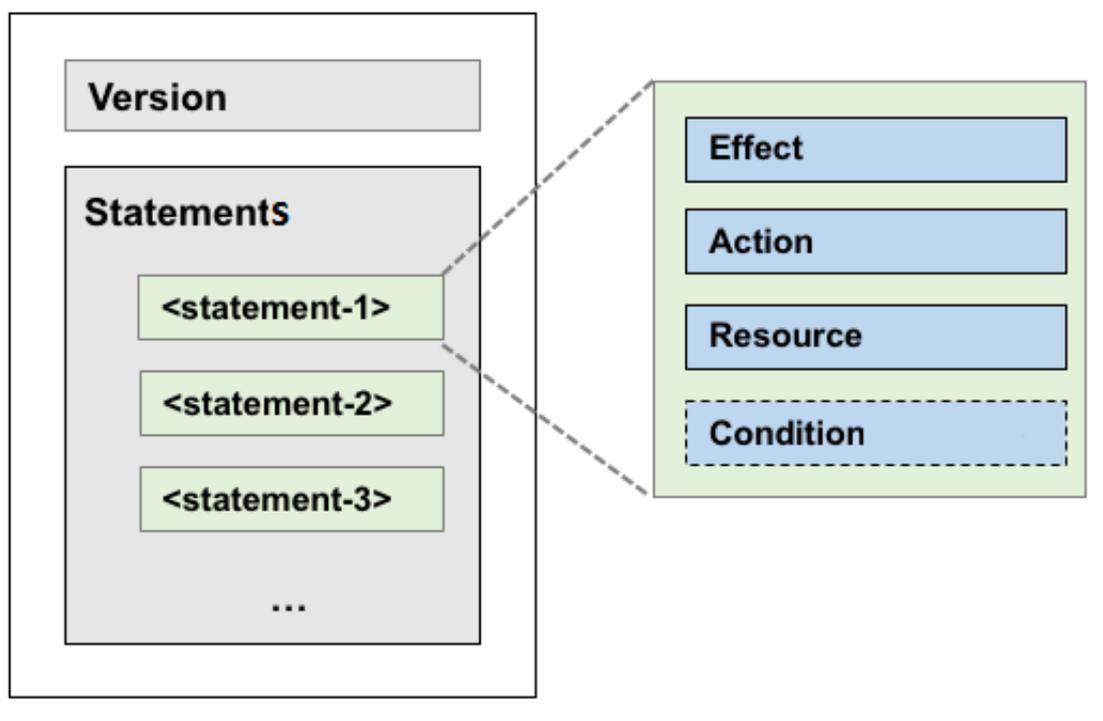
This topic describes the structure, syntax, and rules of policies used in Alibaba Cloud RAM.

Policy structure

The policy structure 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 4-4: Policy structure



Before using a policy syntax

Before using the syntax of a policy, you need to understand its characters and rules.

- Policy characters:
 - The JSON characters in a policy include { } [] " , :.
 - The special characters used to describe the syntax of a policy include = < > () |.
- Rules for using the policy characters:
 - If an element requires multiple values, a comma (,) is used as the delimiter to separate each value, and an ellipsis (...) is used to describe the remaining values. For example, [< action_str ing >, < action_str ing >, ...].

**Note:**

Elements that support multiple values also support single values. This means that the two descriptions " Action ": [< action_str ing >] and " Action ": < action_str ing > 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_blo ck > = " Version " : (" 1 ").

Policy syntax

An example of the syntax of a policy is as follows:

```

policy = {
    < version_blo ck >,
    < statement_ block >
}
< version_blo ck > = " Version " : (" 1 ")
< statement_ block > = " Statement " : [ < statement >, < statement
>, ... ]
< statement > = {
    < effect_blo ck >,
    < action_blo ck >,
    < resource_b lock >,
    < condition_ block ?>
}
< effect_blo ck > = " Effect " : (" Allow " | " Deny ")
< action_blo ck > = (" Action " | " NotAction " ) :
    ("*" | [ < action_str ing >, < action_str ing >, ... ])
< resource_b lock > = (" Resource " | " NotResourc e " ) :
    ("*" | [ < resource_s tring >, < resource_s tring >, ... ])
< condition_ block > = " Condition " : < condition_ map >
< condition_ map > = {
    < condition_ type_strin g > : {

```

```

    < 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 `Allow` or `Deny`.

**Note:**

In a statement, both the action and resource elements can have multiple values.

- Each statement supports its own conditions.

**Note:**

A condition block can contain multiple conditions with different operation types and logical combinations of these conditions.

- **Deny takes effect:** You can grant multiple policies to a user. If these policies 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 ("") such as 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.

Policy format check

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

- For more information 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.

4.4.3 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 : ListObject s` 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 : ListObject s ",
        " oss : GetObject "
      ],
      "Resource": [
        " acs : oss :*:*: mybucket ",
        " acs : oss :*:*: mybucket /*"
      ],
      "Condition": {
        "IpAddress": {
          "acs : SourceIp": [" 42 . 120 . 88 . 10 ", " 42
. 120 . 66 . 0 / 24 " ]
        }
      }
    }
  ]
}
```

```

    }
  ]
}

```

4.5 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.

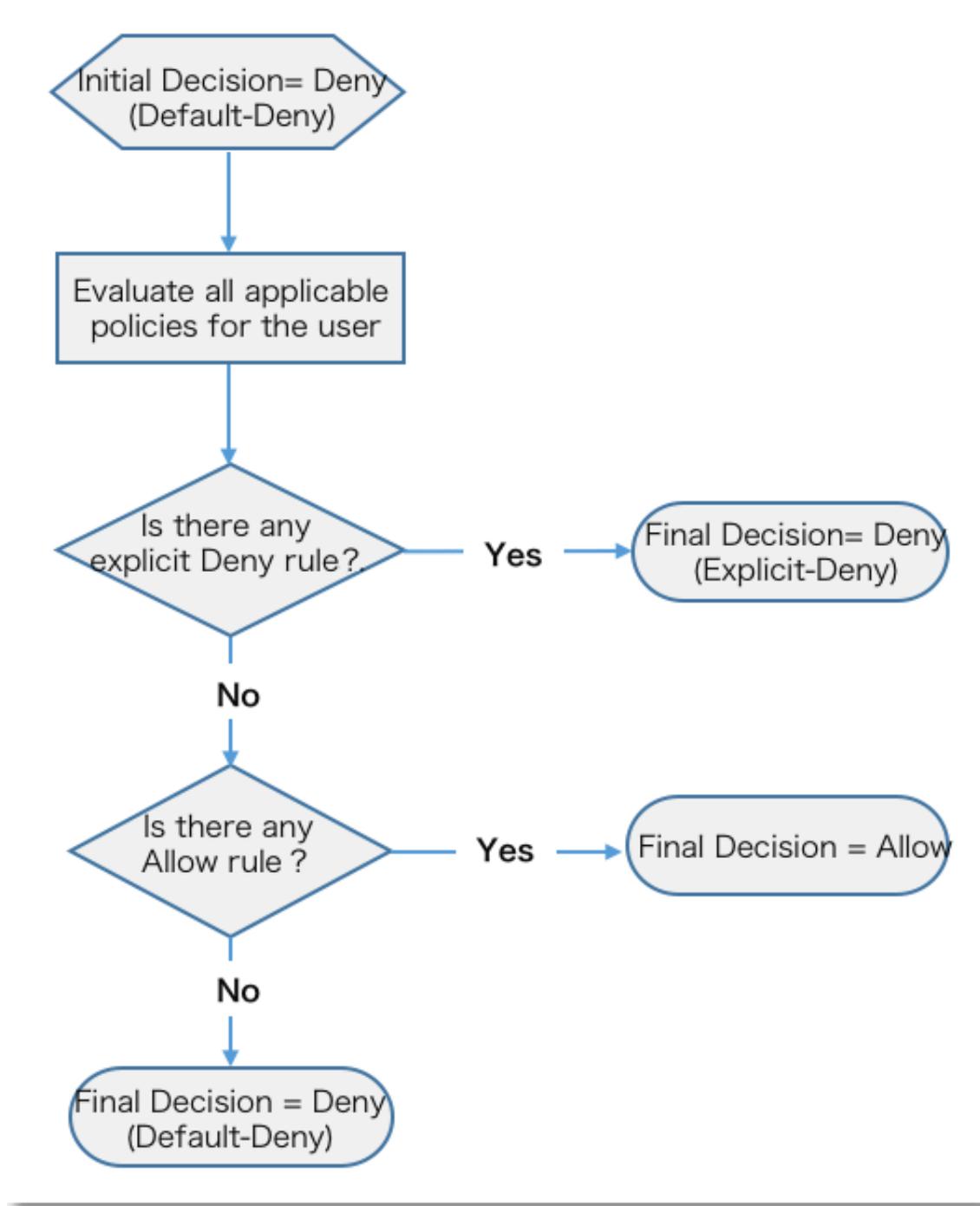
Access type	Rules
Account	<p>The account is the resource owner.</p> <p> Note: Some cloud services, such as Log Service, support cross-account ACL authorization. If the ACL authorization is successful, access is allowed even the account is not the resource owner.</p>
RAM user	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 4-5: 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.

5 Scenarios

5.1 User management and access control

This topic provides an example scenario that describes how to use Alibaba Cloud RAM to manage user permissions and resources.

Scenario

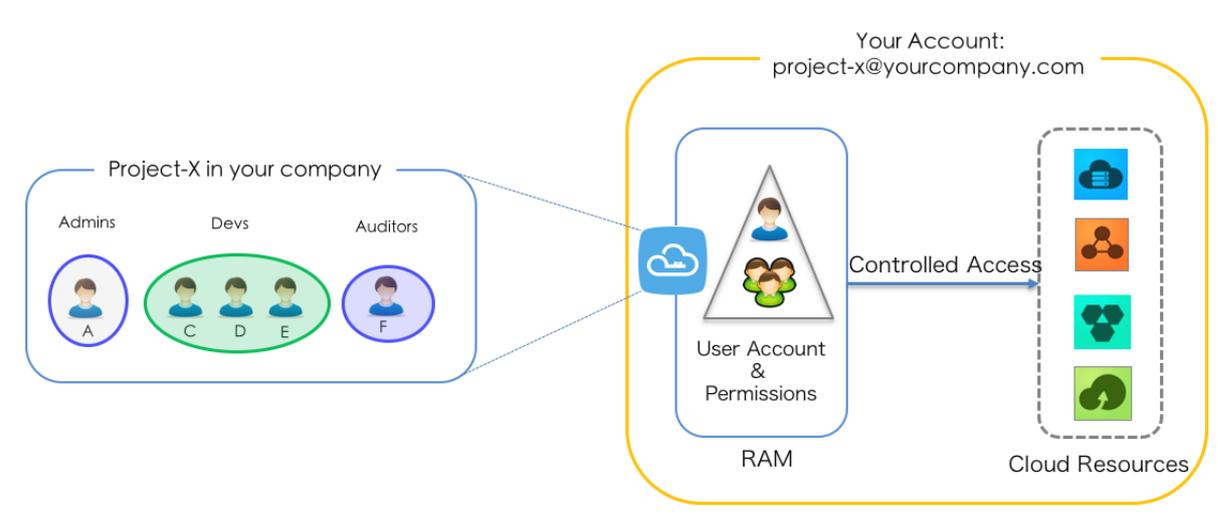
Assume that Enterprise A has bought several types of Alibaba Cloud resources, such as ECS instances, RDS instances, SLB instances, and OSS buckets, for Project-X. In this project, multiple employees need to perform operations on these cloud resources. Specifically, different employees require different permissions to complete different operations.

Requirement analysis

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

Solution

Figure 5-1: Solution



1. Set multi-factor authentication (MFA) to avoid risks associated with mistaken disclosure of the Alibaba Cloud account password. For more information, see [\(Optional\) Set MFA](#).
2. Create RAM users for different employees (or applications) and set logon passwords or create AccessKeys. For more information, see [Create a RAM user](#).
3. 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. For more information, see [\(Optional\) Create a RAM user group](#).
4. Attach one or more system policies to the groups or users. For more information, see [Permission granting in RAM](#). 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](#).

5.2 Grant temporary permissions to mobile apps

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

Scenario

Enterprise A has developed a mobile app, which runs on users' own devices. Therefore, Enterprise A cannot manage these devices directly and wants to use

Alibaba Cloud OSS so that the mobile app can upload data to and download data from OSS.

The requirements of Enterprise A are as follows:

- Enterprise A 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, Enterprise A will not save the AccessKey to the mobile app because mobile devices that run the app are not managed by Enterprise A directly.
- Enterprise A wants to minimize its security risks by granting the app temporary access credentials (by means of an STS token) that the app can then use to connect to OSS, thereby restricting the access duration to a specified period of time.

Solution

- Use the Alibaba Cloud account of Enterprise A (Account A) to create a role in RAM, grant relevant permissions to the role, and allow the appServer (which is logged on as a RAM user) to use this role.

For more information, see [Create a RAM role and user, and grant permissions](#).

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

For more information, see [Obtain and transfer the role STS token and access OSS](#).

- The appServer can further limit the resource operation permissions of the temporary STS token when it assumes the role, to better manage the permissions of each app.

For more information, see [Restrict STS token permissions](#).

Create a RAM role and user, and grant permissions

Assume that the account ID of Account A is 11223344.

1. Account A creates a RAM role `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 more information, see [RAM role management](#).

After creating the role, Enterprise A can view the role information on the basic information page.

- In this example, the Alibaba Cloud Resource Name (ARN) of the role is as follows:

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

- The trust policy in the role (in which only RAM users under Account A can assume) is as follows:

```
{
  "Statement": [
    {
      "Action": "sts : AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs : ram :: 11223344 : root" // If the trusted
          entity type of the role is Alibaba Cloud account
          , 'root' is used by default .
        ]
      }
    }
  ],
  "Version": "1"
}
```

2. Account A attaches the policy `AliyunOSSReadOnlyAccess` (OSS read-only permission) to the role `oss-readonly`.

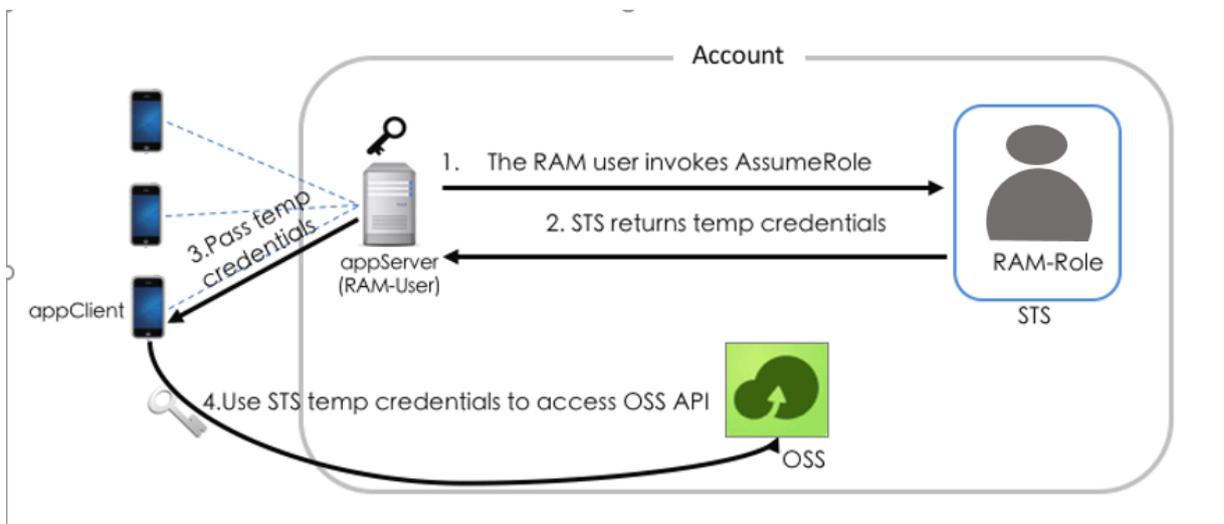
For more information, see [Permission granting in RAM](#).

3. Account A creates a RAM user (here, the RAM user is named Appserver) for the appServer, creates an AccessKey for the RAM user, and attaches the `AliyunSTSAssumeRoleAccess` system policy to the user so that the user can call the STS AssumeRole API.

Obtain and transfer the role STS token and access OSS

The procedure for an app to obtain a role STS token and use it to call the OSS API is illustrated in the following figure.

Figure 5-2: Procedure



The appServer uses the AccessKey of the RAM user Appserver to call the STS API [AssumeRole](#).



Note:

The AccessKey for the appServer must be configured.

The following is an example of how to use aliyuncli to call the AssumeRole API:

```
$ aliyuncli sts AssumeRole -- RoleArn acs : ram :: 11223344 :
role / oss - readonly -- RoleSessionName client - 001
{
  "AssumedRoleUser": {
    "AssumedRoleId": "3915787525_73972854_client - 001",
    "Arn": "acs : ram :: 11223344 : role / oss - readonly /
client - 001"
  },
  "Credentials": {
    "AccessKeySecret": "93ci2umK1Q_KNEja6WGqi_1Ba7Q2Fv9P
wxZqtVF2Vy_nUvz",
    "SecurityToken": "CAES6AIIAR_KAAUiwSHpk_D3GXRMQk9s
tDr3YSVbyG_qanqkS+fPleEkjZ+dLgFnGdCI2_PV93jksolE8ijH8dHJrH
RA5JA1YCGs_fX5hrzcNM3_7Vr4eVdWfV_QhoCw0DXBp_Hv//ZcITp+
ELRr4MHsny_GiErnDsXLk_I7q/sbuWg6PACZ/jzQfEWQb/f7Y1Gh1TVF
MurjEzR2pz_alhUamszOG_RCWTZZeEp0_WEFaayISMz_kxNTc4NzUy
NTcz0Tcy0D_U0Kgpjbgll_bnQtMDAxMK_T+LIHBKjoGUn_NhTUQ1QkoK
ATEaRQoFQW_xsb3cSGwoM_QWN0aW9uRX_F1YWxzEgZB_Y3Rpb24aAw
oBKhIfCg5S_ZXNvdXJjZU_VxdWFscxII_UmVzb3VyY2_UaAwoBKkoF
NDMyNzRSBT_I20DQyWg9B_c3N1bWVkcU9sZVVzZXJg_AGoSMzcxNT
c4NzUyNTcz_0Tcy0DU0cg_lly3MtyWRt_aW544Mbewo/26AE=",
    "Expiration": "2016-01-13T15:02:37Z",
```

```

    " AccessKeyId ": " STS . F13GjskXTj k38dBY6YxJ tXAZk "
  },
  " RequestId ": " E1779AAB - E7AF - 47D6 - A9A4 - 53128708B6 CE "
}

```

Restrict STS token permissions

1. After calling the AssumeRole API, you can grant fine-grained permissions to the STS token.

Specifically, if you do not specify a policy when calling the AssumeRole API, the STS token has all permissions of `oss - readonly`. To solve this issue, you can specify a policy to further restrict the permissions of the STS token, for example, only allow the STS token to access `sample - bucket / 2015 / 01 / 01 /*. jpg`

. The following is an 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 ": " 3915787525 73972854 : client - 002
",
    " Arn ": " acs : ram :: 11223344 : role / oss - readonly /
client - 002 "
  },
  " Credentials ": {
    " AccessKeySecret ": " 28Co5Vyx2X htTqj3RJgd ud4ntyZRSN
dUvNygAj7x EMow ",
    " SecurityToken ": " CAESnQMIAR KAASJgnzMz lXVyJn4KI
+ FsysaIpTgm 8ns8Y74HVE j0p0ev08ZW Xrnnkz4a4r BEPBAdFkh3
197GUspruj siU78Fkszx hnQPkKQKcy vPihoXqKvu ukrQ / Uoudk31KAJ
Ez5o2EjLNU REcxWjRDRS ISMzKxNTc4 NzUyNTcz0T cy0DU0Kgpj
bGllbnQtMD AxMKmZxIHB KjoGUnNhTU Q1Qn8KATEa egoFQWxsB3
cSJwoMQWN0 aW9uRXF1YW xzEgZBY3Rp b24aDwoNb3 Nz0kdldE9i
amVjdBJICg 5SZXNvdXJj ZUVxdWFscx IIUmVzb3Vy Y2UaLAoqYW
NzOm9zczoq Oio6c2FtcG xllWJ1Y2tl dC8yMDE1Lz AxLzAxLyout
anBnSgU0Mz I3NFIFMjY4 NDJaD0Fzc3 VtZWRSb2xl VXNlcmAAah
Iz0TE1Nzg3 NTI1NzM5Nz I4NTRYCWVj cy1hZG1pbm jgxt7Cj / boAQ
==" ,
    " Expiration ": " 2016 - 01 - 13T15 : 03 : 39Z ",
    " AccessKeyId ": " STS . FJ6EMcS1JL ZgAcBJSTDG 1Z4CE "
  },
  " RequestId ": " 98835D9B - 86E5 - 4BB5 - A6DF - 9D3156ABA5 67 "
}

```



Note:

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 obtains and parses the credentials.

- The appServer obtains the AccessKeyId, AccessKeySecret, and STS token 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 transfers the STS token to the app.

4. The app uses the STS token to directly access APIs of Alibaba Cloud services (such as OSS).

The following is an example of how to use aliyuncli and an STS token to access an OSS object (here, the STS token is issued to client-002):

```
Configure the STS token syntax : aliyuncli oss Config
-- host -- accessid -- accesskey -- sts_token
$ aliyuncli oss Config -- host oss . aliyuncs . com --
accessid STS . FJ6EMcS1JL ZgAcBJSTDG 1Z4CE -- accesskey
28Co5Vyx2X htTqj3RJgd ud4ntyZrSN dUvNygAj7x EMow -- sts_token
CAESnQMIAR KAASJgnzMz lXVyJn4KI + FsysaIpTGm 8ns8Y74HVE
j0p0evO8ZW Xrnnkz4a4r BEPBA dFkh3 197GUspruj siU78Fkszx
hnQPKkQKcy vPihoXqKvu ukrQ / Uoudk31KAJ Ez5o2EjLNU REcxWjRDRS
ISMzkxNTc4 NzUyNTcz0T cyODU0Kgpj bGllbnQtMD AxMKmZxIHB
KjoGUnNhTU Q1Qn8KATEa egoFQWxs b3 cSJwoMQWN0 aW9uRXF1YW
xzEgZBY3Rp b24aDwoNb3 NzOkdl dE9i amVjdBJICg 5SZXNvdXJj
ZUVxdWFscx IIUmVzb3Vy Y2UaLAoqYW NzOm9zczoq Oio6c2FtcG
xLLWJ1Y2tl dC8yMDE1Lz AxLzAxLy anBnSgU0Mz I3NFIFMjY4
NDJaD0Fzc3 VtZWRSb2xl VXNlcmAAah Iz0TE1Nzg3 NTI1Nz M5Nz
I4NTRYCWVj cy1hZG1pb n jgxt7Cj / boAQ ==
access OSS objects
$ aliyuncli oss Get oss :// sample - bucket / 2015 / 01 / 01
/ grass . jpg grass . jpg
```

What to do next

For more information, see:

- [Set up direct data transfer for mobile apps](#)
- [Permission control](#)
- [Set up data callback for mobile apps](#)
- [STS temporary access authorization](#)

5.3 Cross-account resource authorization and access

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

Scenario

Account A and Account B represent two different enterprises (Enterprise A and Enterprise B, respectively). Enterprise A has bought various cloud resources (such as ECS instances, RDS instances, SLB instances, and OSS buckets) to support its business

.

Requirement analysis

- Account A is the resource owner and wants to grant Account B the relevant permissions to perform operations on resources of Account A.
- Account B wants to further grant the permissions to its RAM users (employees or applications). If an employee of Account B joins or leaves Enterprise B, Account A cannot make any changes to the permissions.
- If Enterprise A or Enterprise B ends the agreement, Account A can remove the permissions of Account B at any time.

Solution

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

- Account A creates a role in RAM, grants relevant permissions to the RAM role, and allows Account B to use this role.

For more information, see [Cross-account authorization](#).

- If an employee (that is, a RAM user) under Account B needs to use this role, Account B can grant permissions to this RAM user to perform operations on the resources of Account A.

For more information, see [Cross-account resource access](#).

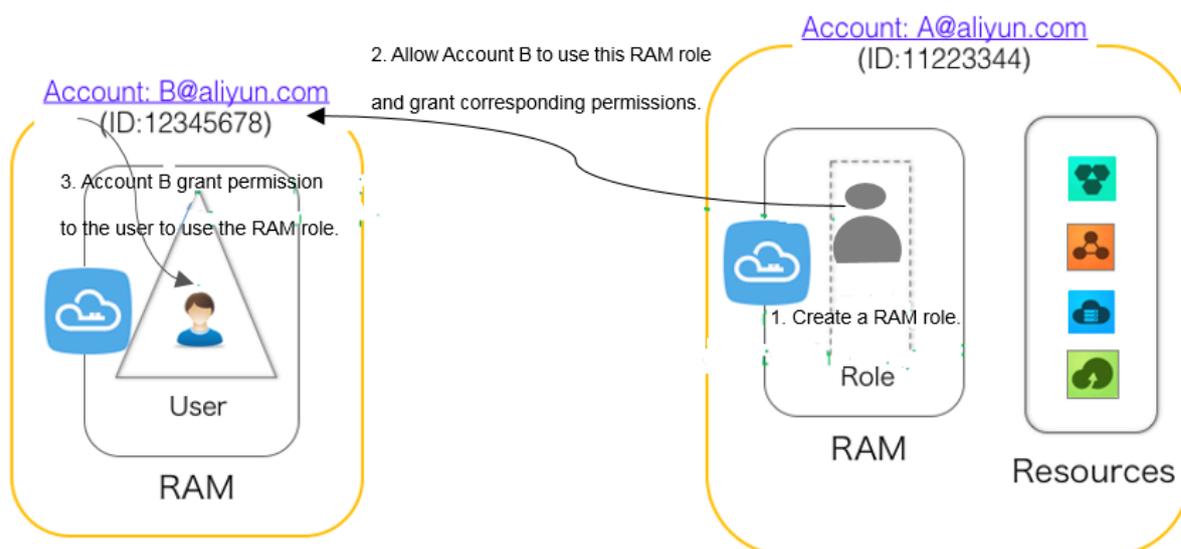
- If Enterprise A or Enterprise B ends the agreement, Account A can revoke the permissions of Account B. In this case, all RAM users of Account B lose the permissions associated with this role.

For more information, see [Removing cross-account authorization](#).

Cross-account authorization

The following figure shows how to use a RAM role to achieve cross-account authorization. In this example, Enterprise A (whose account ID is 11223344 and account alias is company-a) needs to grant ECS operation permissions to the employees of Enterprise B (whose account ID is 12345678 and account alias is company-b).

Figure 5-3: Use a RAM role to achieve cross-account authorization



- Account A creates a RAM role (here, the role is named `ecs-admin`) and selects Other Alibaba Cloud Account (here, the account ID is 12345678) as a trusted entity.

For more information, see [RAM role management](#).

After creating the role, Account A can view the role information on the Basic Information page.

- In this example, the Alibaba Cloud Resource Name (ARN) of the role is as follows:

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

- The trust policy in the role (in which only RAM users under Account B can assume) is as follows:

```
{
  "Statement": [
    {
      "Action": "sts : AssumeRole",
      "Effect": "Allow",
```

```
" Principal ": {
  " RAM ": [
    " acs : ram :: 12345678 : root "
  ]
}
],
" Version ": " 1 "
}
```

2. Account A attaches the `AliyunECSF ullAccess` policy to the role `ecs-admin`.

For more information, see [Permission granting in RAM](#).

3. Account B creates a RAM user (here, the RAM user is named Alice) for its employee, sets a logon password for the RAM user, and attaches the `AliyunSTSA ssumeRoleA ccess` system policy for the RAM user to call the STS AssumeRole API.

Cross-account resource access

To allow RAM user Alice under Account B to access the ECS resources of Account A (through the Alibaba Cloud console), follow these steps:

1. Log on to the RAM console.

During logon, enter the account alias `company-b`, RAM user name `Alice`, and password `123456`.

2. Move the pointer over the account icon and click `Switch Role`.

On the displayed page, enter `company-a` for `Enterprise Alias/Default Domain Name` and `ecs-admin` for `Role Name`.



Note:

After completing the preceding operations, the RAM user Alice can perform operations on the ECS resources of Account A.

Removing cross-account authorization

If Account A wants to remove the permission of using the role `ecs-admin` from Account B, the procedure is as follows:

1. Log on to the RAM console, click `RAM Roles`, and click the role name of `ecs-admin`.

2. Click the Trust Policy Management tab and delete `acs : ram :: 12345678 : root`.

**Note:**

Account A can also remove the permission of using the role `ecs-admin` from Account B by deleting the `ecs-admin` role on the RAM Roles page. However, the role cannot have any policies attached to it before being deleted.

5.4 Dynamic identity and permission management of cloud applications

This topic describes how to use Alibaba Cloud RAM to allow applications to access Alibaba Cloud APIs by obtaining the dynamic STS token of a RAM role.

Scenario

An enterprise has bought ECS instances and wants to deploy its applications in ECS. To allow the applications to access other Alibaba Cloud APIs by using AccessKeys, the enterprise can use one of the following methods:

- Embed the AccessKeys into the code.
- Save the AccessKeys in the configuration files of the applications.

However, if the preceding methods are used, the following issues occur:

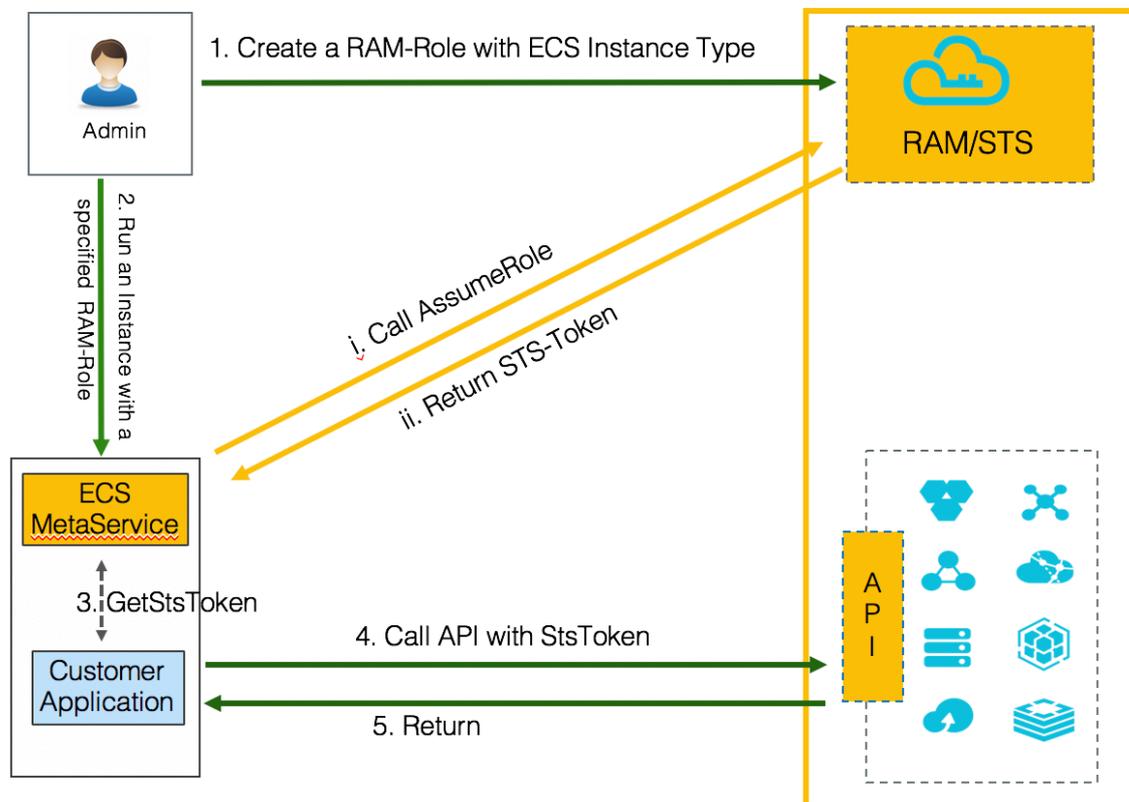
- **AccessKey disclosure:** If the AccessKeys are embedded in the ECS instances in plaintext, they can be mistakenly disclosed to another user due to the sharing of a snapshot, or an image to create a shared image instance.
- **O&M complexity:** If the AccessKeys are changed (due to AccessKey rotation or changes to user identities), all instances and images need to be updated and redeployed because the AccessKeys exist in the ECS instances. As a result, the management of instances and images is highly complex.

Solution

To resolve the preceding issues, you can combine ECS with the access control feature of 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.

Figure 5-4: Process



Configure a RAM role for an ECS instance

1. The administrator uses the Alibaba Cloud account to create an ECS instance RAM role and attach appropriate policies to the RAM role.



Note:

An ECS instance RAM role is a type of RAM service role that is created by a user and used by the ECS instance of the user after authorization.

2. The administrator starts the ECS instance and configures the RAM role.
 - (i) ECS calls the AssumeRole API according to the configured RAM role to access STS and sends a request to obtain the STS token of the RAM role.
 - (ii) STS verifies the identity of ECS and the policies attached to the RAM role. If the verification succeeds, a STS token is issued. If the verification fails, the request is denied.

For more information, see [Use the instance RAM role in the console](#) or [Use the instance RAM role by calling APIs](#).

3. Upon obtaining the STS token, the ECS instance provides the STS token to its applications through the 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>
```



Note:

- The applications can call Alibaba Cloud APIs when the STS token is within the validity period. The STS token usually expires after one hour. ECS automatically refreshes the STS token before it expires.
- 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.

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



Note:

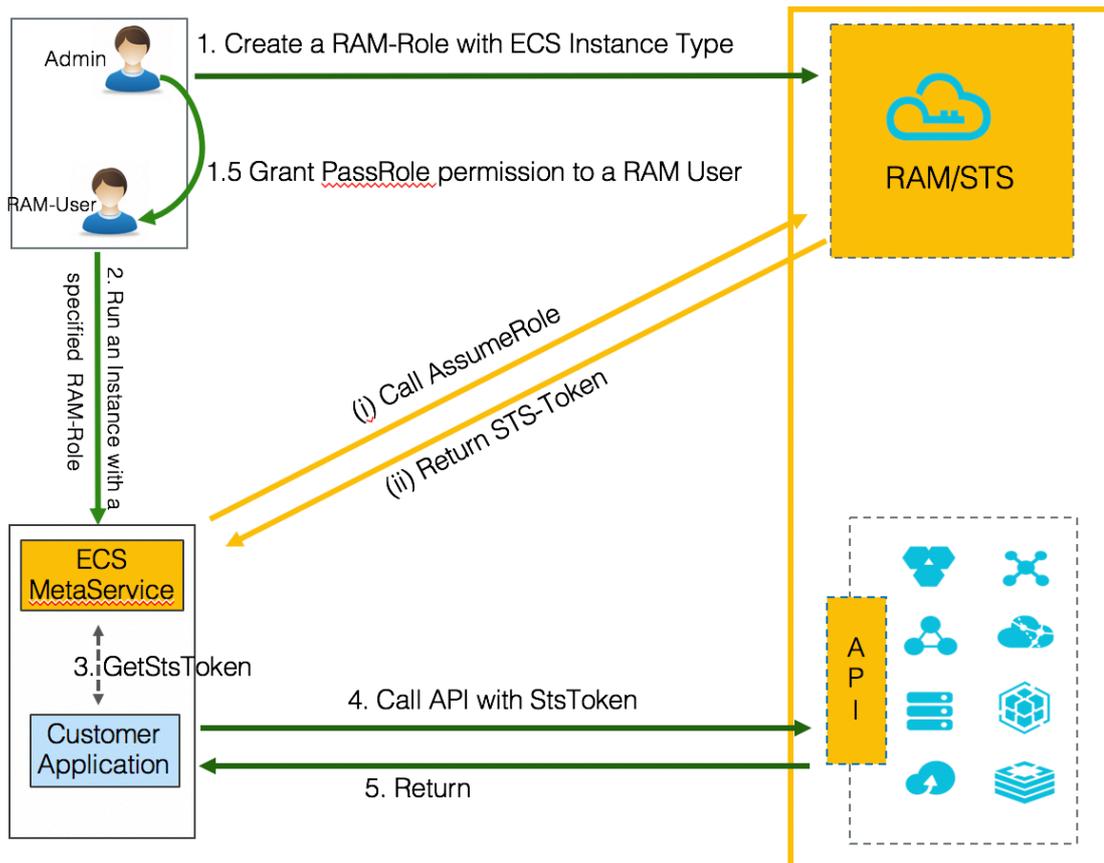
If the applications use Alibaba Cloud SDK, the Alibaba Cloud SDK can obtain the STS token of the RAM role from the ECS Metadata service, and the developers do not need to configure any sensitive AccessKey-related information in the SDK.

For more information, see [Configure RamRole to achieve non-AccessKey access to ECS instances](#).

Separate permissions of administrators and general users

In most scenarios, the permissions of the administrator and a typical ECS instance user are configured as different RAM users. The following figure shows how to separate the permissions of the administrator and a general user.

Figure 5-5: Process



Notice:

- 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 a RAM role, ECS checks whether the RAM user has the `ram : PassRole` permission of the RAM role. If no permission is found, the RAM user cannot create an ECS instance.
- Only authorized users can configure RAM roles for ECS instances. In this way, the use of RAM roles is strictly controlled, which helps to prevent any abuse of permission usage.

To separate the permissions of the administrator and the general user, you need to [configure a RAM role for an ECS instance](#) and grant the `PassRole` permission to the general user, as shown in Step 1.5 in the preceding figure.

The administrator can also create a custom policy and attach the policy to the general user. The following is an example:

**Notice:**

The `rolename` must be replaced with the RAM name.

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

What to do next

If Alibaba Cloud RAM does not meet all of your permission application requirements, you can use other Alibaba Cloud services, such as Function Compute and MaxCompute, that provide the access control features to help manage the identities and AccessKeys of your users and applications on the cloud.

5.5 Use an externally authorized account to log on to Alibaba Cloud

This topic describes how to authenticate the identity of an internal enterprise account before the internal account is used to access Alibaba Cloud resources.

Scenario

Enterprise A has two departments that use Alibaba Cloud resources. Each department has its own Alibaba Cloud account (named as A1 and A2). Enterprise A also has its own domain account system, namely Microsoft Active Directory (AD) and Active Directory Federation Services (AD FS).

Enterprise A has strict requirements on identity access management:

- All operations on Alibaba Cloud must pass identity authentication through the domain account system of Enterprise A. All employees are prohibited from using independent accounts and passwords to access the cloud resources.
- Enterprise A 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

Relevant concepts

The following table describes the concepts relevant to this solution.

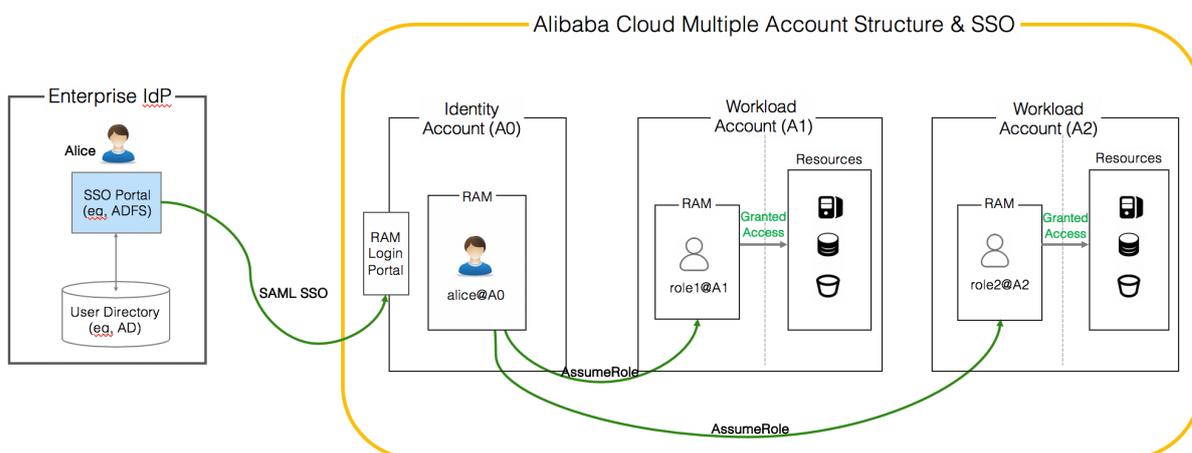
Concept	Description
Workload Account	Purchases Alibaba Cloud resources, such as ECS instances, RDS, and OSS.
Identity Account	Creates only RAM users under an Alibaba Cloud account.
Service Provider	Uses the identity management function of an IdP to provide users with specific service applications. An SP uses the user information provided by an Identity Provider (IdP).

If an enterprise has two Workload Accounts, follow these steps:

1. Create an independent Identity Account.
2. Use the Identity Account as a service provider and integrate it with the local IdP to implement Single Sign On (SSO).

- Use the cross-account access function provided by Alibaba Cloud through RAM roles to authorize its RAM users (employees) to access the resources under other Alibaba Cloud accounts.

Figure 5-6: Process



Procedure

- Register a new Alibaba Cloud account and use it as an Identity Account (A0).



Note:

A0 is used to resolve issues concerning user synchronization and SSO.

- Use the account A0 to log on to the RAM console and configure SSO.
- In the AD FS of the enterprise, add A0 as a service provider.
- Synchronize local domain users who need to access the cloud resources to RAM.
- Use the Workload Account A1 to log on to the RAM console, create a RAM role (RAM role 1) in Workload Account A1 that can be used for cross-account authorization, grant required permissions to RAM role 1, and set A0 as the trusted Alibaba Cloud account.
- Use the Workload Account A2 to log on to the RAM console, create a RAM role (RAM role 2) in Workload Account A2 that can be used for cross-account authorization, grant required permissions to RAM role 2, and set A0 as the trusted Alibaba Cloud account.
- Grant the RAM users under the Identity Account A0 the permission to assume RAM role 1 or RAM role 2.