Alibaba Cloud
Resource Access Management

SSO Management

Issue: 20190917

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

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

Contents

Legal disclaimer..... I
Generic conventions..... I
1 SSO overview.....1
2 Application scenarios of SSO.....3
3 User-based SSO.....4
3.1 Overview of user-based SSO.....4
3.2 Configure the SAML for user-based SSO..... 6
3.3 Configure the SAML of an IdP during user-based SSO.....7
3.4 Implement user-based SSO by using AD FS.....10
4 Role-based SSO..... 20
4.1 Overview of role-based SSO.....20
4.2 Identity providers..... 23
4.2.1 Create an identity provider..... 23
4.2.2 View basic information about an identity provider.....23
4.2.3 Modify basic information about an identity provider..... 24
4.2.4 Delete an identity provider..... 24
4.3 Configure the SAML for role-based SSO..... 24
4.4 Configure the SAML of an IdP during role-based SSO..... 25
4.5 SAML assertions for role-based SSO.....27
4.6 Implement role-based SSO by using AD FS..... 30
4.7 Implement role-based SSO by using Azure Active Directory.....43
5 Best practices..... 58
5.1 Use RAM to maintain security of your Alibaba Cloud resources..... 58

1 SSO overview

This topic describes the concepts and methods of Single Sign On (SSO), also known as identity federation. Enterprises can implement SSO to their Alibaba Cloud accounts by using SAML 2.0.

Concepts

Identity provider (IdP)	A RAM entity that provides identity management services. IdPs are generally classified into the following types: · 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)	An application that uses the identity management function of an IdP to provide users with specific services. An SP uses the user information provided by an IdP. In some identity systems (such as OpenID Connect) that do not comply with the SAML protocol, SP is known as relying party, which means the relying party of an IdP.
Security Assertion Markup Language 2.0 (SAML 2.0)	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 enterprise-level SSO.
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 IdPs (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 #unique_4.
- 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 #unique_5.

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 #unique_6.

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 #unique_8.
- Your IdP does not support complex configuration of attributes.
- You want to simplify IdP configuration.

3 User-based SSO

3.1 Overview of user-based SSO

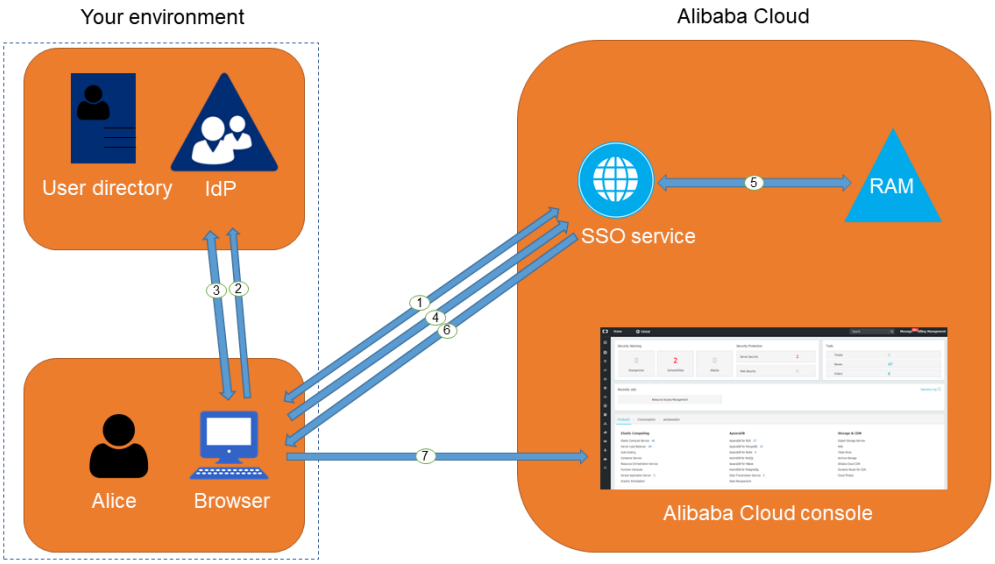
This topic describes the scenario, process, and configuration of user-based Single Sign On (SSO).

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 service provider (SP) and the enterprise system is the identity provider (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 preceding 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 #unique_11.
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 #unique_12.
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 #unique_13.

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 #unique_14.

3.2 Configure the SAML for user-based SSO

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

Prerequisites

A default domain name, a domain alias, or an auxiliary domain name is set to simplify SAML SSO. For more information, see #unique_16 and #unique_17.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click SSO.
3. Click the User-based SSO tab.
4. In the SSO Settings section, click Modify to modify the SSO settings as needed.
   - SSO Status: You can enable or disable the SSO function as needed.

     Note:
     This setting applies to all RAM users under your Alibaba Cloud account.

     - The SSO function is disabled by default. If 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 by using passwords is automatically displayed.
   - 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.

- Auxiliary Domain: (Optional) You can turn on or turn off this function as needed.
  - If you turn on this function, you can set an auxiliary domain name and use it as the suffix of the `NameID` element in the SAML assertion.
  - If you turn off this function, you can only use the default domain name or domain alias of your Alibaba Cloud account as the suffix of the `NameID` element in the SAML assertion.

  For more information about values of the `NameID` element, see #unique_12.

  Note:
  If you set a domain alias and an auxiliary domain name at the same time, only the domain alias or the default domain name can be used as the suffix of the `NameID` element.

What's 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 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 Single Sign On (SSO). You can configure Alibaba Cloud as a trusted SAML service provider (SP), and configure an SAML assertion in the IdP.

Procedure

1. Obtain the SAML SP metadata URL from Alibaba Cloud.
   a) Log on to the RAM console by using your Alibaba Cloud account.
   b) In the left-side navigation pane, click SSO.
   c) Click the User-based SSO tab.
   d) Copy the SAML SP metadata URL.
2. Create an SAML SP in your IdP and then configure Alibaba Cloud as the relying party by using one of the following methods:
   - Copy and paste the SAML SP metadata URL of Alibaba Cloud into your IdP.
   - If your IdP does not support URL configuration, click Copy 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.
   - If you fail to upload an XML file to your IdP, configure the following parameters:
     - `EntityID`: The value of the `entityID` attribute in the `md:EntityDescriptor` element of the metadata XML file.
     - `ACSURL`: The value of the `Location` attribute in the `md:AssertionConsumerService` element of the metadata XML file.
     - `RelayState`: Optional. If the `RelayState` parameter is available in your IdP, you can set this parameter to the URL to be directed after SSO succeeds. If this parameter is left unspecified, the home page of the Alibaba Cloud console is directed after SSO succeeds.

     Note:
     Only the URL in the `*.console.aliyun.com` or `*.console.alibabacloud.com` domain can be set for `RelayState`.

What's next

After you configure Alibaba Cloud as a trusted SAML SP, you need to 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` element in the SAML assertion, then matches the `NameID` element to the UPN of the corresponding RAM user, so that user-based SSO 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` element in the SAML assertion. The `NameID` element must contain one of the following suffixes:

- The domain alias of your Alibaba Cloud account, for example, `< username >@< domain_alias >`. Here, the <username> sub-element is the username of a RAM user, and the `< domain_alias >` sub-element is the domain alias. For information about how to set a domain alias, see #unique_17.
- The auxiliary domain name that is set for user-based SSO, for example, `< username >@< auxiliary_domain >`. Here, the <username> sub-element is the username of a RAM user, and the `< auxiliary_alias >` sub-element is the auxiliary domain name. For information about how to set an auxiliary domain name, see Set an auxiliary domain name.

  > **Note:**
  > If you set a domain alias and an auxiliary domain name at the same time, only the domain alias can be used as the suffix of the `NameID` element.

- The default domain name of your Alibaba Cloud account, for example, `< username >@< default_domain >`. Here, the <username> sub-element is the username of a RAM user, and the `< default_domain >` sub-element is the default domain name. For information about how to set a default domain name, see #unique_16.

  > **Note:**
  > You can use the default domain name of your Alibaba Cloud account as the suffix of the `NameID` element regardless of whether you set a domain alias or an auxiliary domain name.

Assume that you have a RAM user named `Alice`, and the default domain name of your Alibaba Cloud account is `example.onaliyun.com`.

- If you set the domain alias of your Alibaba Cloud account to `example.com`, the `NameID` element in the SAML assertion is `Alice@example.onaliyun.com` or `Alice@example.com`.
- If you do not have a domain alias and set the auxiliary domain name to `example2.com`, the `NameID` element in the SAML assertion is `Alice@example.onaliyun.com` or `Alice@example2.com`.

- If you set the domain alias of your Alibaba Cloud account to `example.com` and the auxiliary domain name to `example2.com`, the `NameID` element in the SAML assertion is `Alice@example.onaliyun.com` or `Alice@example.com`.

3.4 Implement user-based SSO by using AD FS

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

Notes

This topic uses Windows Server 2012 R2 as an example to describe how to implement user-based SSO from AD FS 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.

Example configuration

The configuration details used in the example are as follows:

- The default domain name of the Alibaba Cloud account: `secloud.onaliyun.com`.
- The RAM user under the Alibaba Cloud account: `alice`. The User Principal Name (UPN) of the RAM user is `alice@secloud.onaliyun.com`.
- The AD FS of the on-premises Microsoft AD: `adfs.secloud.club`.
- The domain name of the on-premises Microsoft AD: `secloud.club`. The NETBIOS is `secloud`.

- The UPN of the RAM user (Alice) in Microsoft AD: `alice @ secloud . club` .

  The RAM 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
```

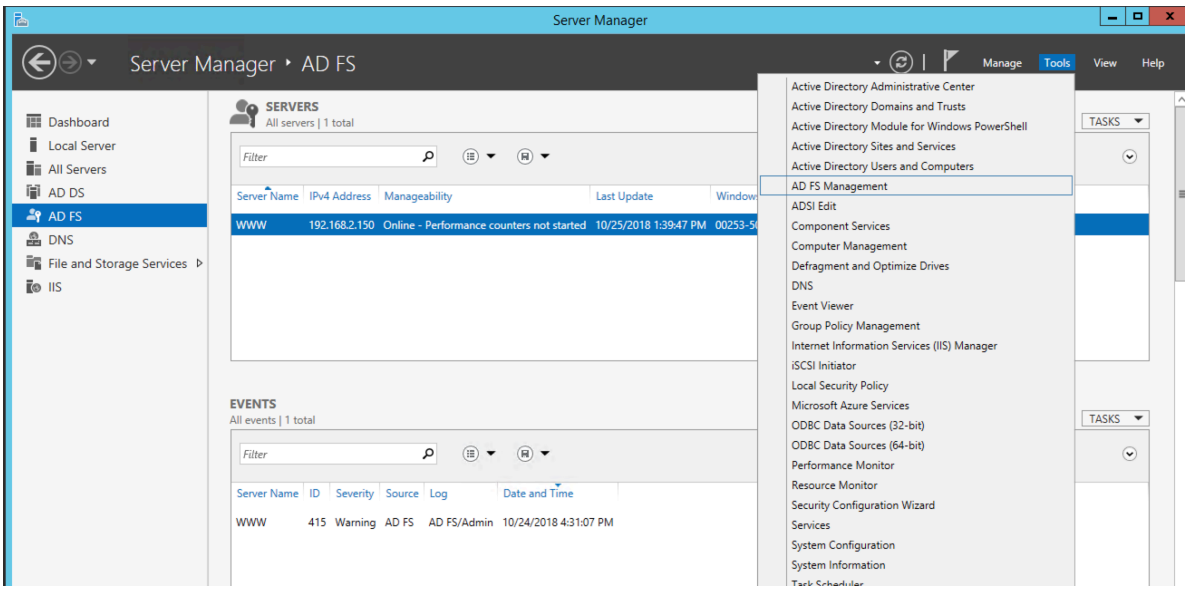
2. Download the metadata file in XML format.
3. In the RAM console, use the metadata file for SSO configuration.

For more information, see #unique_11.

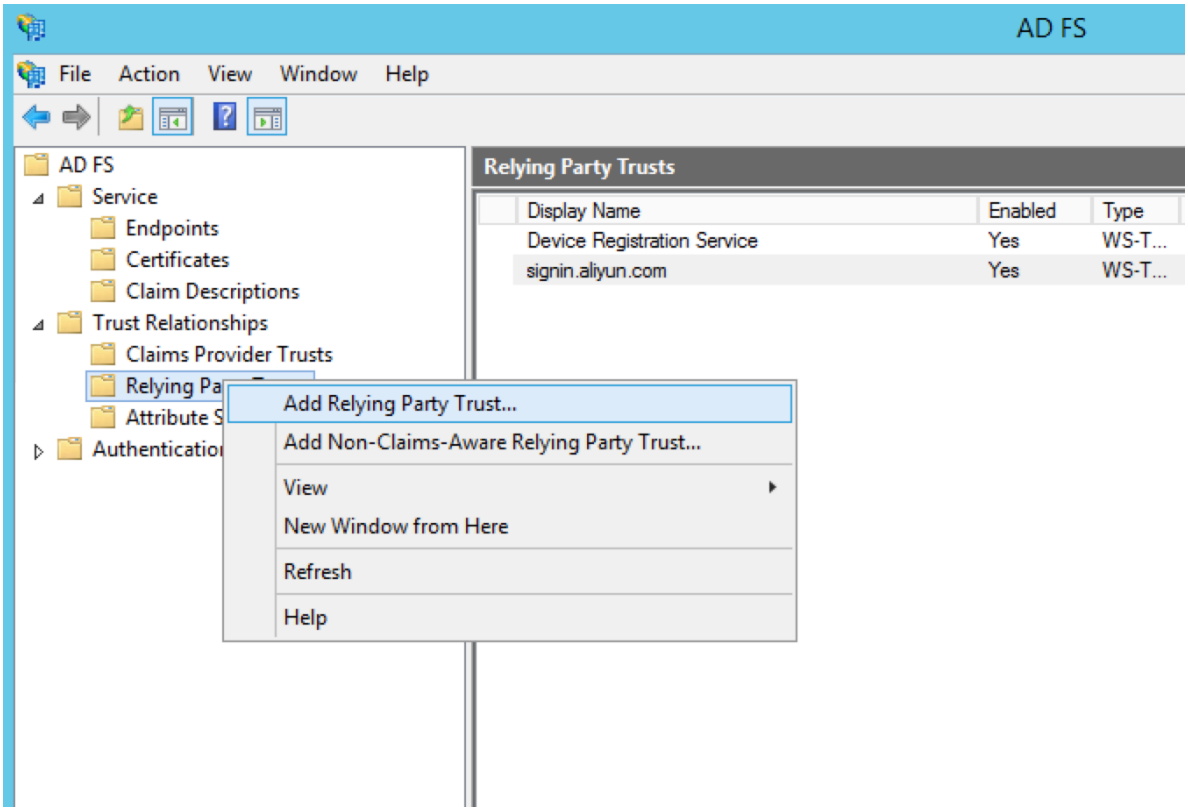
Configure Alibaba Cloud as a trusted SAML SP in AD FS

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.

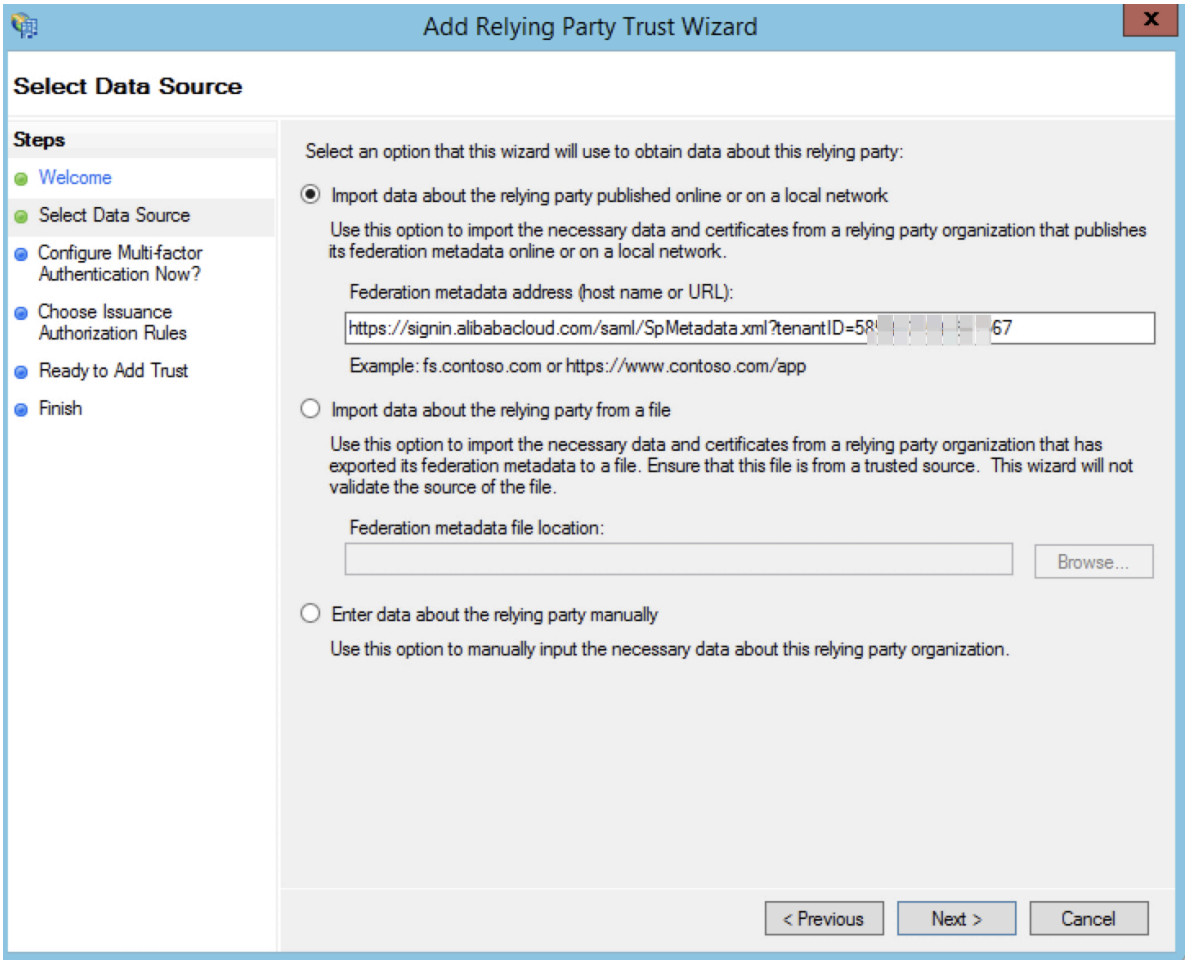


2. Select Add Relying Party Trust.



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

   To view the SAML metadata URL, log on to the RAM console, click 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.



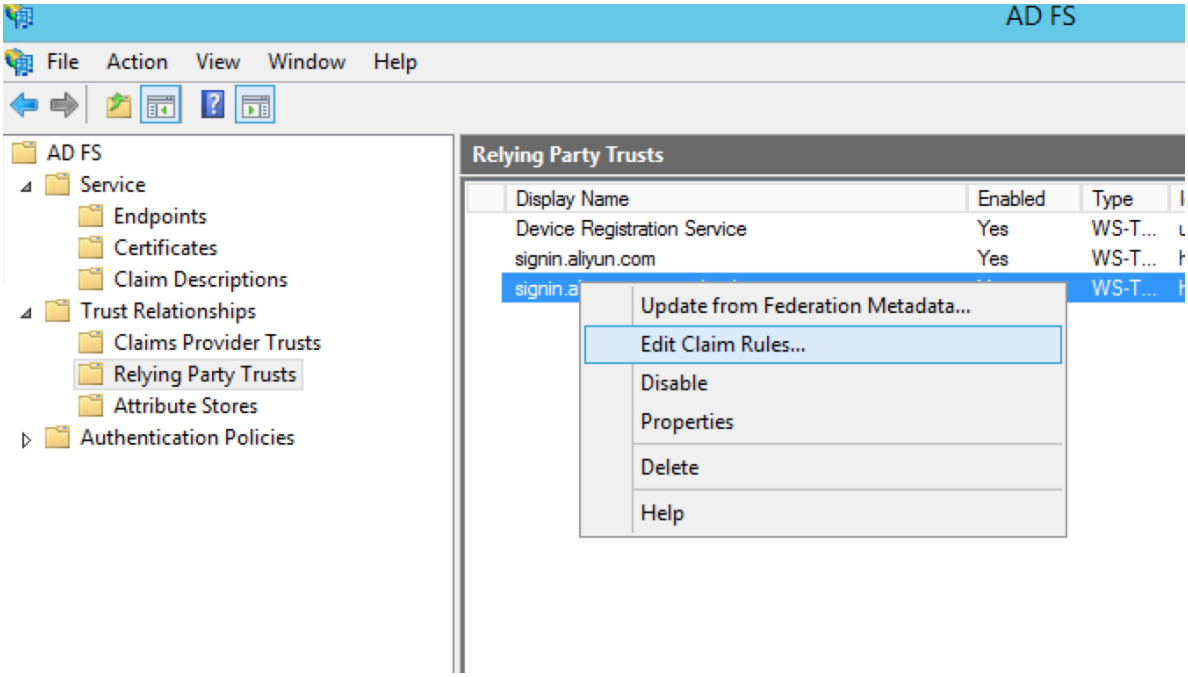
   After the relying party is configured, Alibaba Cloud sends a request to authenticate RAM users under the Alibaba Cloud account whose default domain name is `secloud.onaliyun.com` to AD FS `adfs.secloud.club`. AD FS receives the request from Alibaba Cloud, authenticates the user, and sends a response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

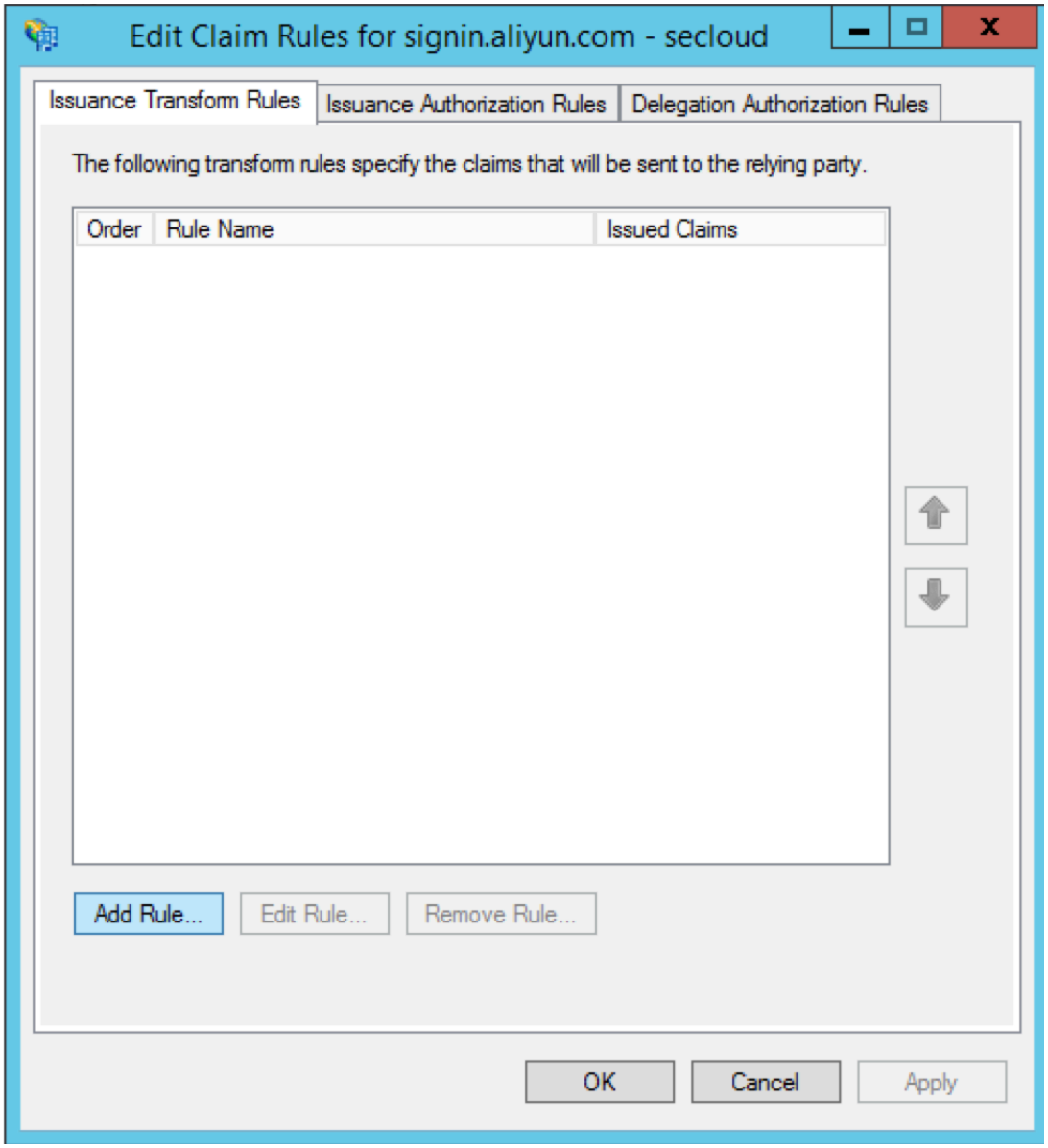
1. Right-click the display name of the relying party and select Edit Claim Rules.



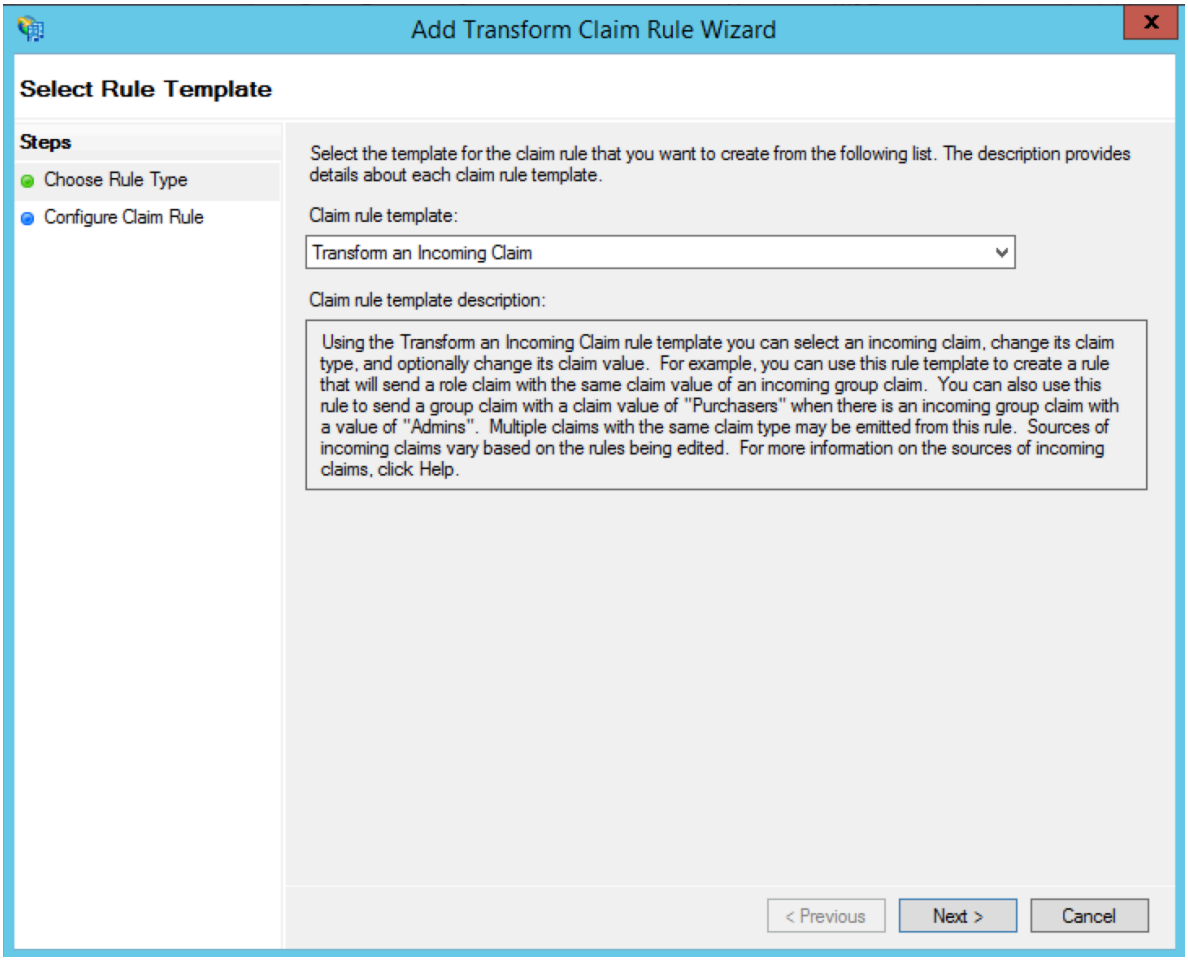
2. Click Issuance Transform Rules to add a rule.

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.



4. Select Edit Rule.

> **Note:**
>
> In this example, the domain name of the UPN in the Alibaba Cloud account is `secloud.onaliyun.com`, and the domain name of the UPN in Microsoft AD

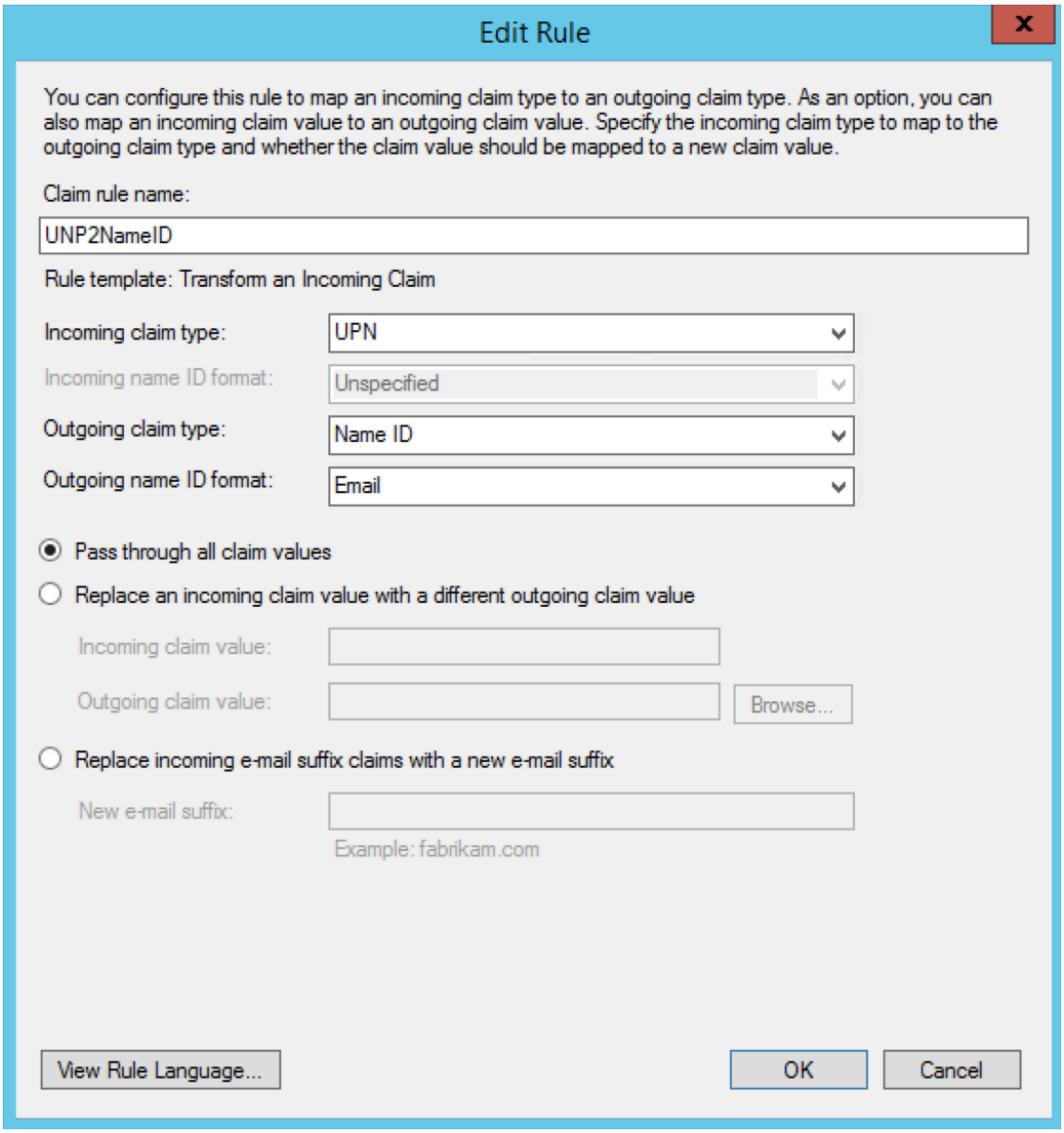
is `secloud.club`. If you directly map the UPN in Microsoft AD to the `NameID`, Alibaba Cloud cannot match the correct user.

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

a. Method 1: Set the domain name of Microsoft AD to the domain alias of your Alibaba Cloud account.

   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 information about how to set a domain alias, see #unique_17.

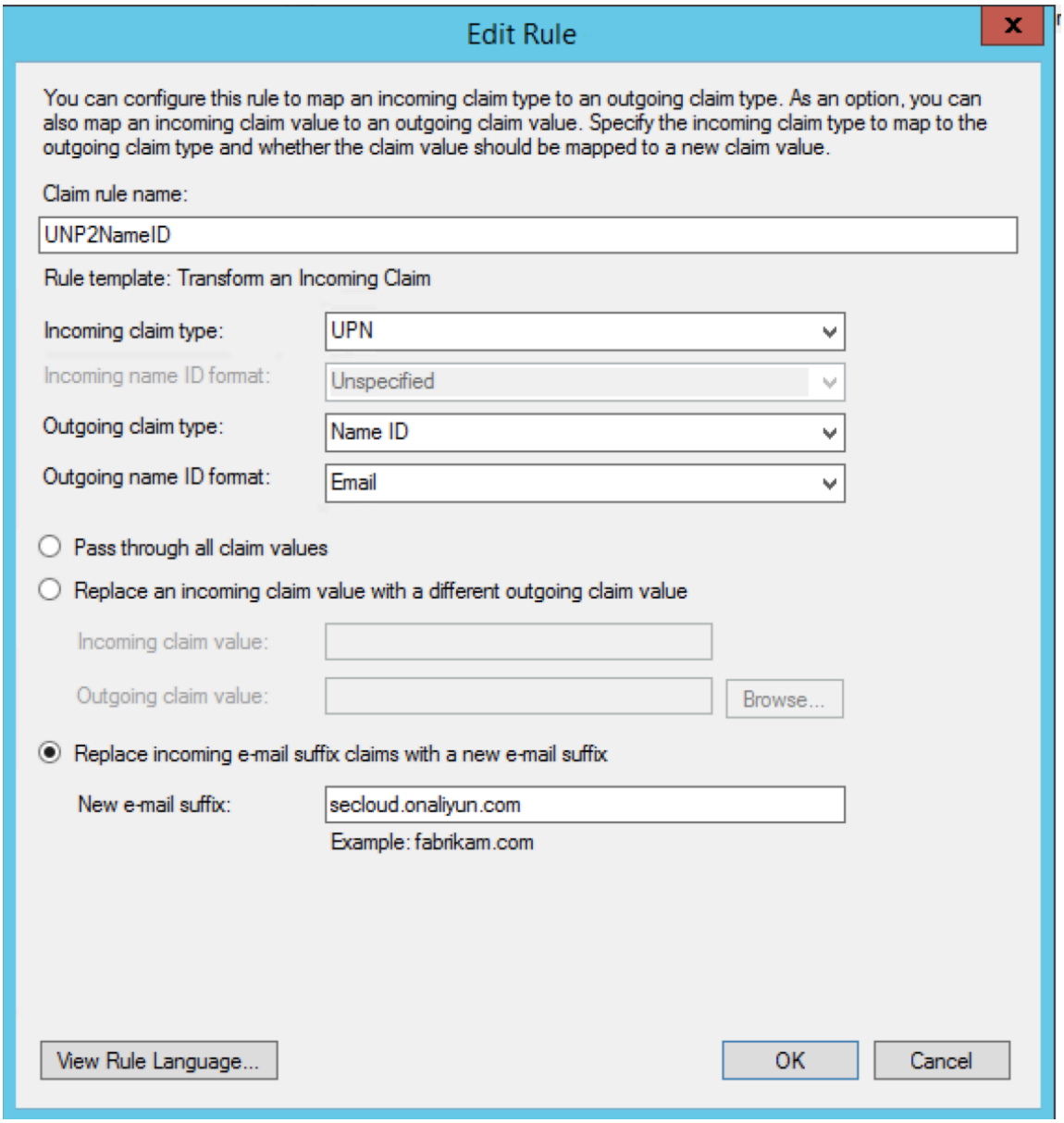
   After the settings are completed, map the UPN to the `NameID` on the Edit Rule page.



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

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

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



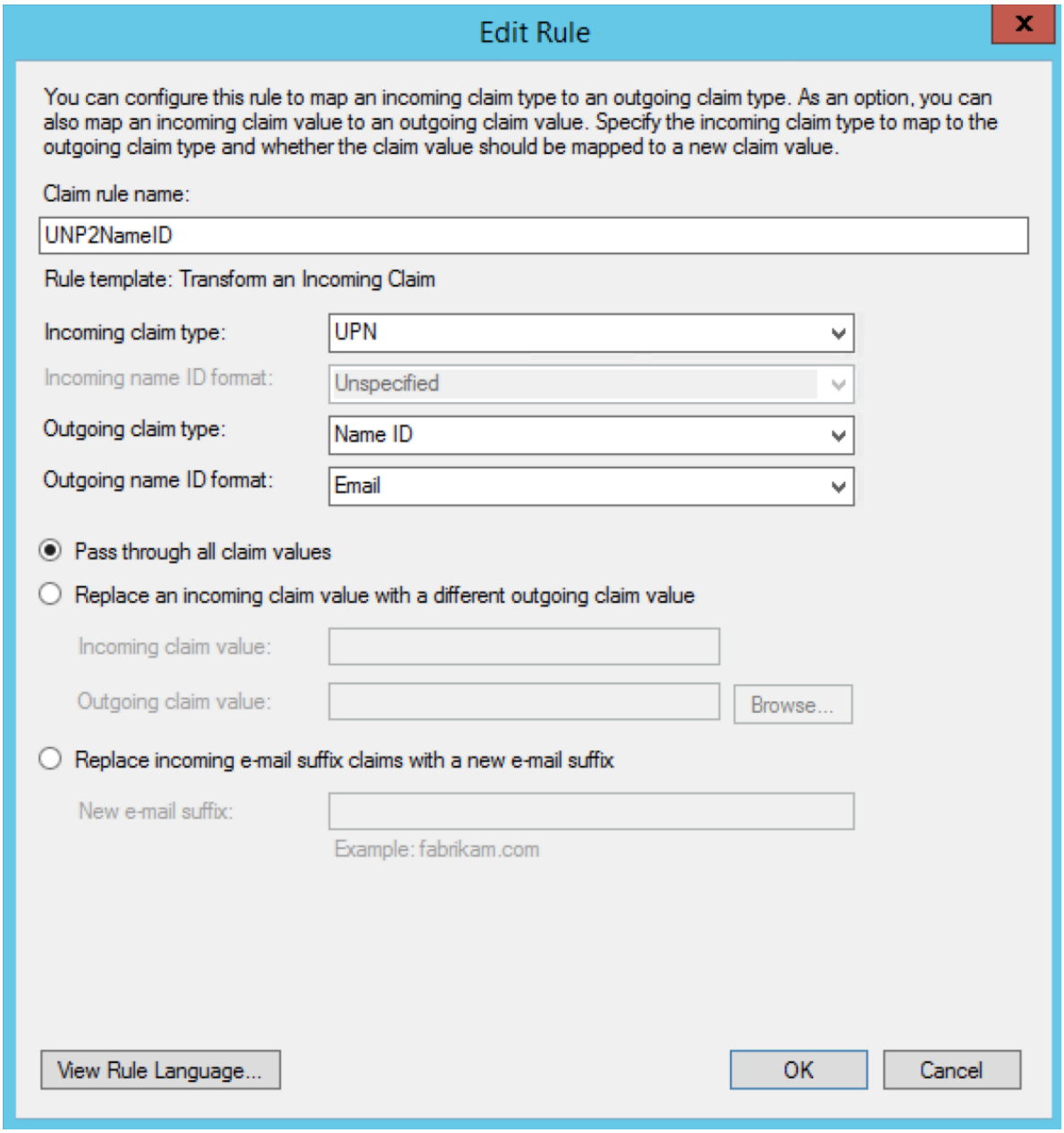
c. Method 3: Set the domain name of Microsoft AD to an auxiliary domain name.

Note:

You can configure auxiliary domain by modifying SSO settings on the User-based SSO tab.

If the domain name `secloud.club` is an intranet domain name of an enterprise, Alibaba Cloud cannot verify the domain ownership of the enterprise. In this case, you can set `secloud.onaliyun.com` to the auxiliary domain name. For information about how to set an auxiliary domain name, see Set an auxiliary domain name.

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



4 Role-based SSO

4.1 Overview of role-based SSO

This topic describes the scenario, process, and configuration of role-based Single Sign On (SSO).

Scenario

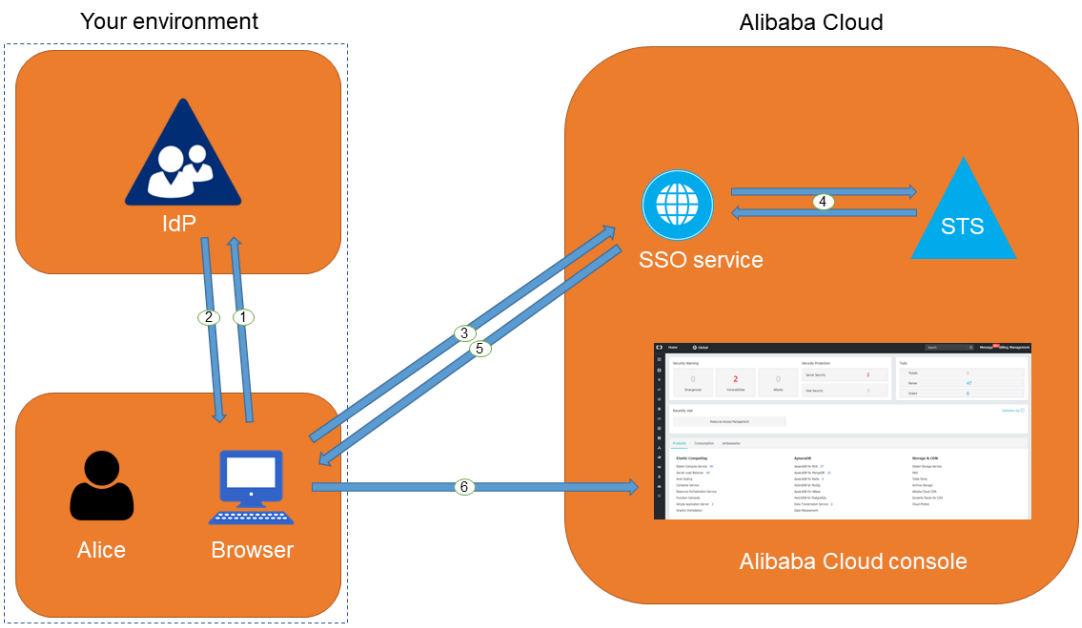
In scenarios where Alibaba Cloud and the identity management system of an enterprise work together to perform role-based SSO, Alibaba Cloud is the service provider (SP) and the enterprise system is the identity provider (IdP). Through role-based SSO, the enterprise can manage users in the local IdP without synchronizing users from your IdP to Alibaba Cloud, and the enterprise employee can log on to Alibaba Cloud by 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 4-1: 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 the 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 :// ADFSServic eName / adfs / ls / IdpInitiat edSignOn . aspx` .

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

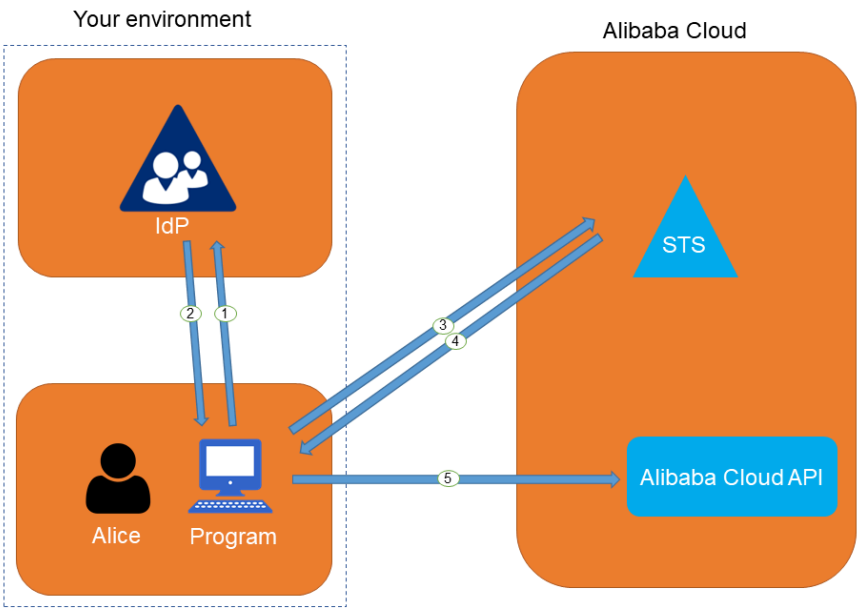
2. The IdP generates an SAML response to the browser.
3. The browser redirects to the page of the SSO service, and forwards the SAML response.
4. The SSO service uses the SAML response to request an STS token from the Alibaba Cloud STS service, and generates a URL that can log on to the Alibaba Cloud 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 4-2: 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 an SAML response that contains the user's SAML assertion, and returns the SAML response to the program.
3. The program calls the #unique_22 API action of the Alibaba Cloud STS service, and forwards the information including the ARN of an Alibaba Cloud IdP, the ARN of the role to be assumed, and the SAML assertion obtained from the IdP.
4. The 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.

Configure role-based SSO

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 #unique_23.

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 #unique_24.

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 #unique_25.

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 #unique_26.

4.2 Identity providers

4.2.1 Create an identity provider

This topic describes how to create an identity provider (IdP). You must create an IdP before you use role-based Single Sign On (SSO).

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, click Create IdP.
4. Enter an IdP name and description.
5. In the Metadata File section, click Upload to upload a metadata file.

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

6. Click OK.

4.2.2 View basic information about an identity provider

This topic describes how to view basic information about an identity provider (IdP), such as the IdP name and the Alibaba Cloud Resource Name (ARN) of the IdP.

Procedure

1. Log on to the RAM console.

2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, click the name of the target IdP.
4. In the IdP Information section, view the IdP information.

4.2.3 Modify basic information about an identity provider

This topic describes how to modify basic information about an identity provider (IdP), such as the IdP description and the metadata file.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, click the name of the target IdP.
4. In the IdP Information section, click Modify.

> Note:
> The IdP name cannot be modified.

5. Click OK.

4.2.4 Delete an identity provider

This topic describes how to delete an identity provider (IdP) that you no longer need. After you delete your IdP, you cannot perform Single Sign On (SSO) between your enterprise and Alibaba Cloud RAM.

Procedure

1. Log on to the RAM console.
2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, find the target IdP and click Delete.
4. Click OK.

4.3 Configure the SAML for role-based SSO

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

Procedure

1. Log on to the RAM console.

2. In the left-side navigation pane, click SSO.
3. On the Role-based SSO tab, click Create IdP.
4. Enter an IdP name and description.
5. In the Metadata File section, click Upload to upload a metadata file.

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

6. Click OK.

What's next

After you create 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 #unique_24.

4.4 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 Single Sign On (SSO). You can configure Alibaba Cloud as a trusted SAML service provider (SP), and configure SAML assertions in the IdP.

Procedure

1. Obtain the SAML SP metadata URL `https://signin.alibabacloud.com/saml-role/sp-metadata.xml`.
   a) Log on to the RAM console by using your Alibaba Cloud account.
   b) In the left-side navigation pane, click SSO.
   c) On the Role-based SSO tab, copy the SAML SP metadata URL.

2. Create an SAML SP in your IdP and configure Alibaba Cloud as the relying party by using one of the following methods:
   - Copy and paste the SAML SP metadata URL of Alibaba Cloud into your IdP.
   - If your IdP does not support URL configuration, click Copy 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.
   - If you fail to upload an XML file to your IdP, configure the following parameters:
     - `Entity ID`: `urn:alibaba:cloudcomputing:international`
     - `ACS URL`: `https://signin.alibabacloud.com/saml-role/sso`
     - `RelayState`: Optional. If the `RelayState` parameter is available in your IdP, you can set this parameter to the URL to be directed after SSO succeeds. If this parameter is left unspecified, the home page of the Alibaba Cloud console is directed after SSO succeeds.

       Note:
       Only the URL in the `*.console.aliyun.com` or `*.console.alibabacloud.com` domain can be set for `RelayState`.

What's next

After you configure Alibaba Cloud as a trusted SAML SP, you must configure SAML assertions in your IdP.

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

For more information about SAML assertions, see #unique_34.

4.5 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 an 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 "> administra  tor </ NameID >

  < SubjectCon  firmation   Method =" urn : oasis : names : tc :
 SAML : 2 . 0 : cm : bearer ">
    < SubjectCon  firmationD  ata   NotOnOrAft  er =" 2019 -
 01 - 01T00 : 01 : 00 . 000Z "  Recipient =" https :// signin .
 alibabaclo  ud . com / saml - role / sso "/>
  </ SubjectCon  firmation >
</ 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 : cloudcompu  ting : internatio  nal
 </ Audience >
  </ AudienceRestriction >
</ Conditions >
```

Custom elements required by Alibaba Cloud

The `AttributeStatement` 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.aliyun.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`

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 . aliyun . com / SAML - Role / Attributes / SessionDur ation`

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

  The value of `AttributeV alue` 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 `SessionDur ation` sub-element:

```
< Attribute   Name =" https :// www . aliyun . com / SAML - Role /
 Attributes / SessionDur  ation ">
  < AttributeV  alue > 1800 </ AttributeV  alue >
</ Attribute >
```

4.6 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.

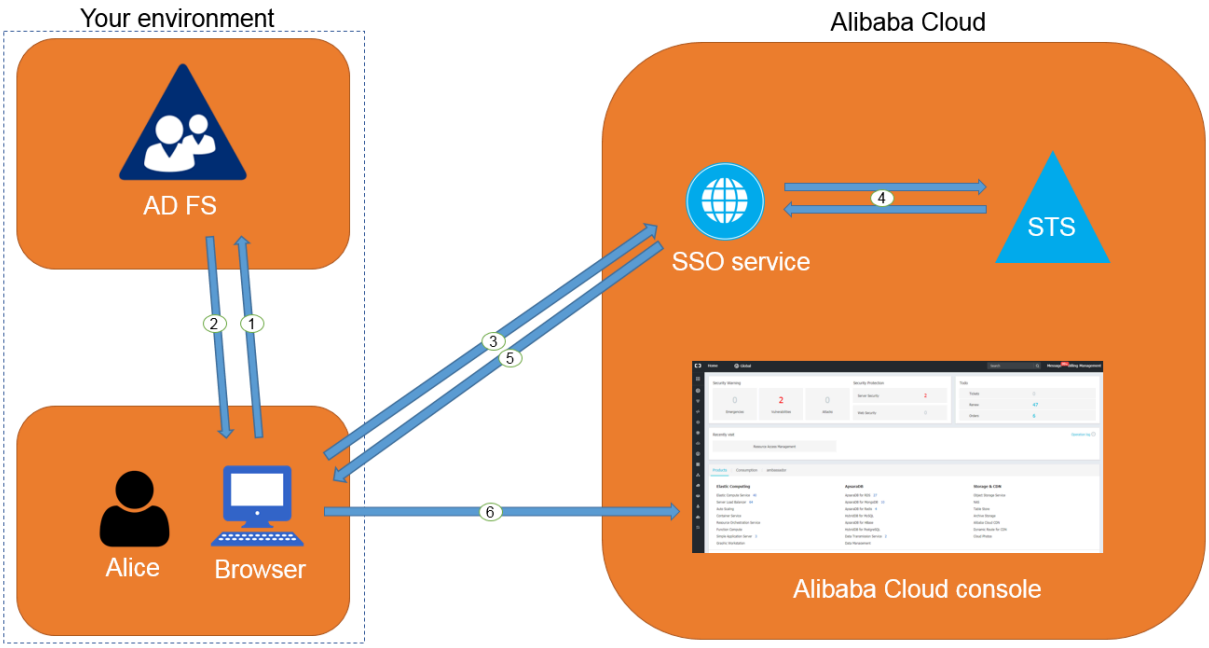
Scenario

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 #unique_5.

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://<ADFS-server>/federationmetadata/2007-06/federationmetadata.xml`.

     Note:

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

For more information, see #unique_23.

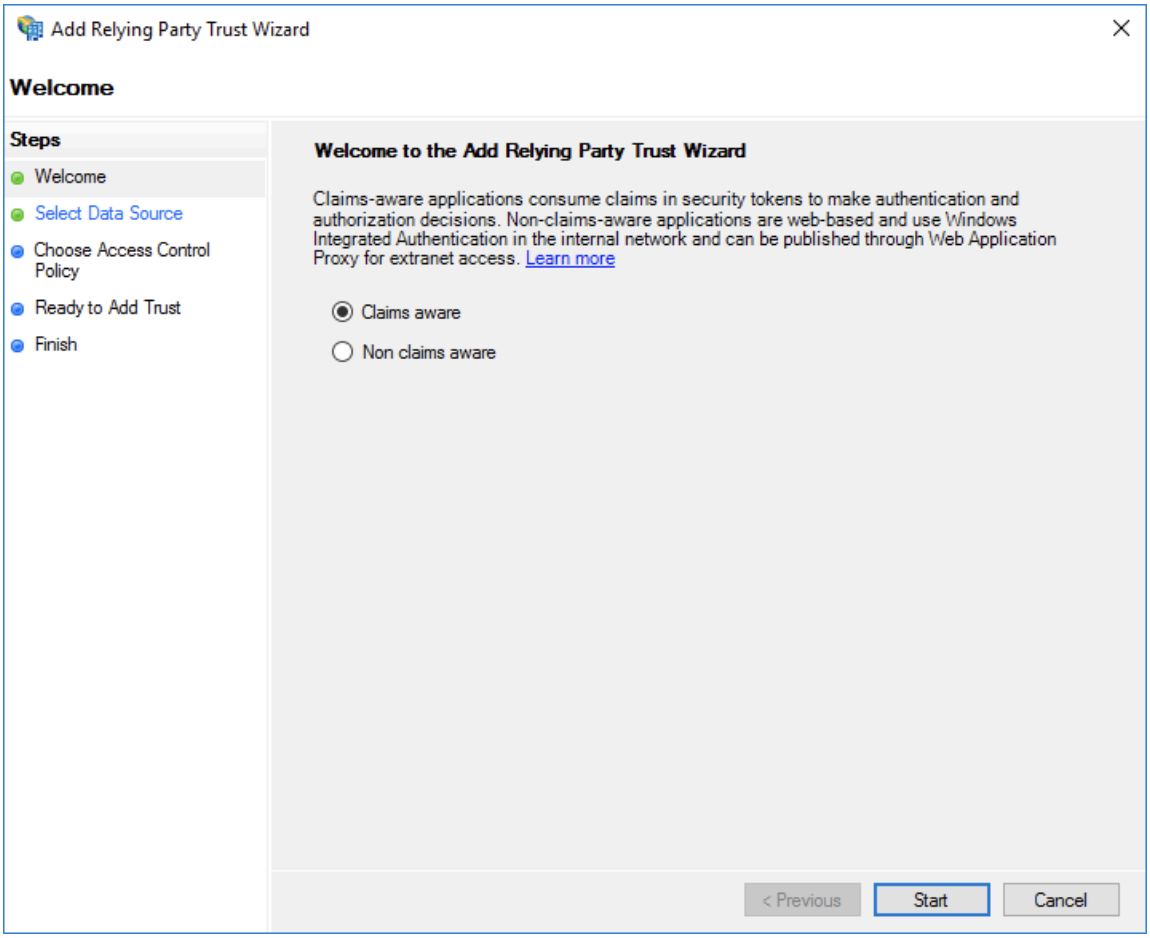
2. Create two RAM roles named ADFS-Admin and ADFS-Reader under Account1, select `ADFS` you have created as the trusted entity, and attach the `AdministratorAccess` and `ReadOnlyAccess` policies to these two RAM roles respectively. For more information, see #unique_37.
3. Create an IdP and two RAM roles 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.

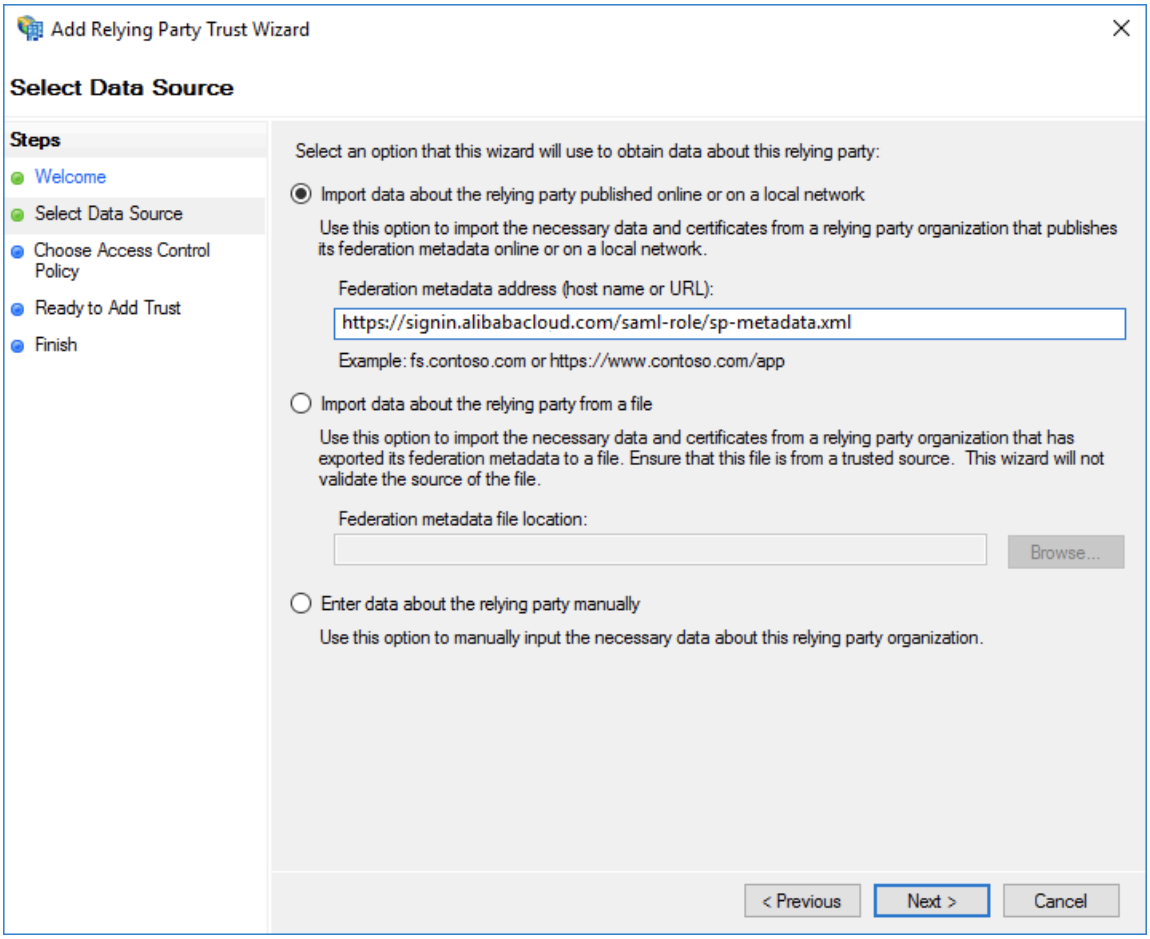
- Configure Alibaba Cloud as a trusted SAML SP in AD FS.

  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`.



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`

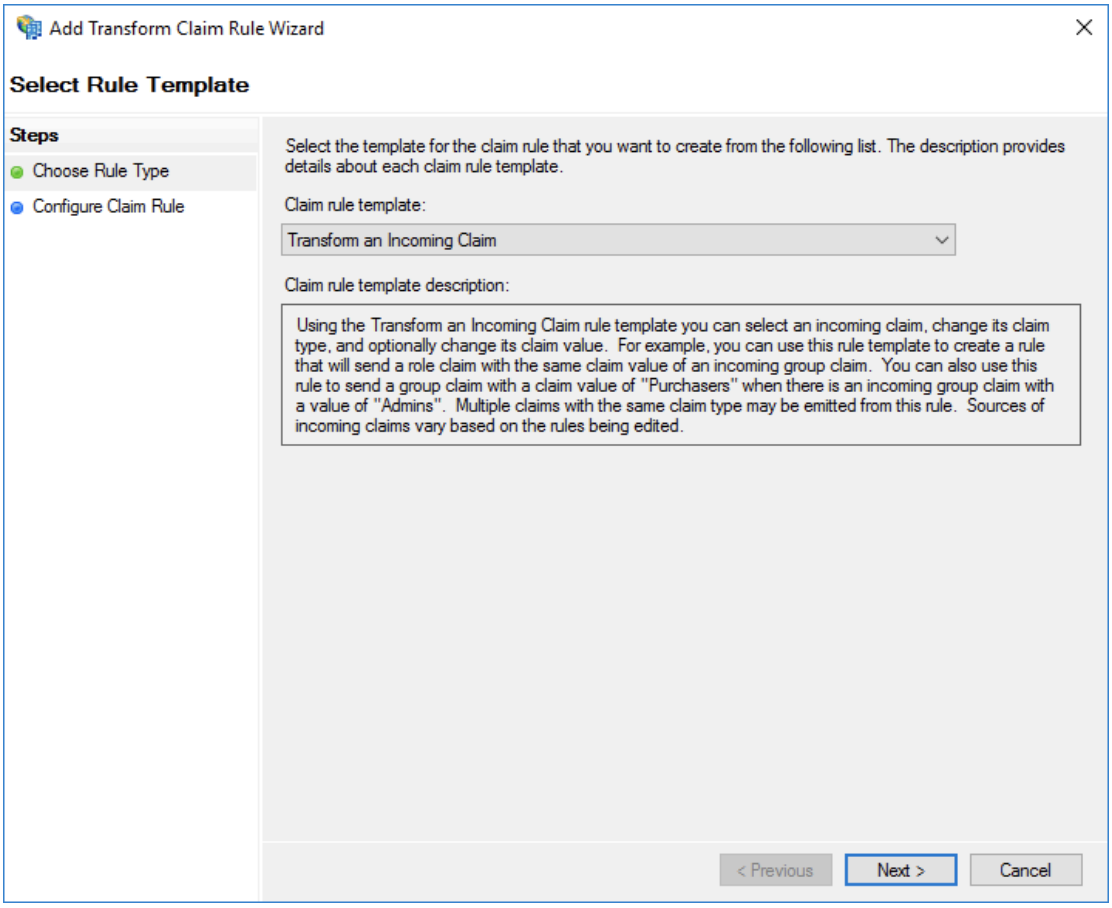
    Follow these steps to configure the Windows account name of AD to be the `NameID` in the SAML assertion:

    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

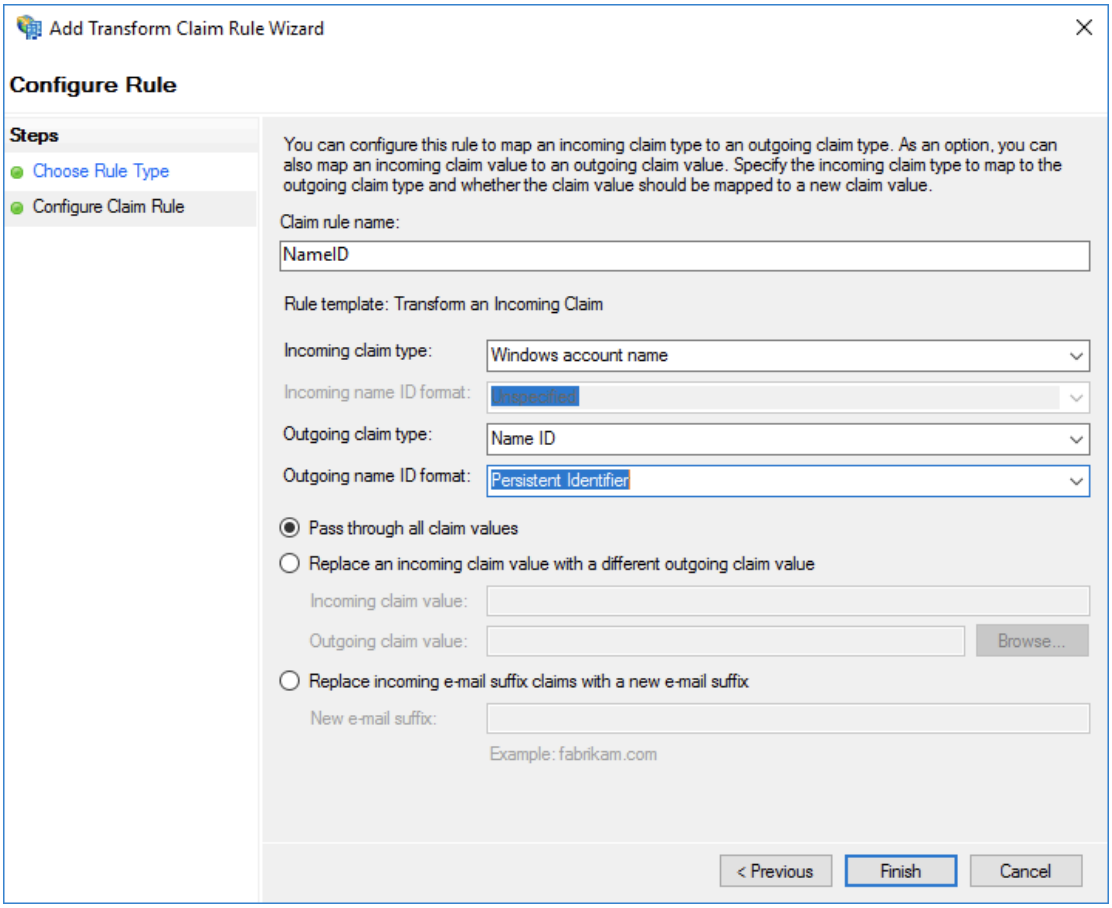
Windows account name of a user in AD as a `NameID`. This means that a new rule is required.

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



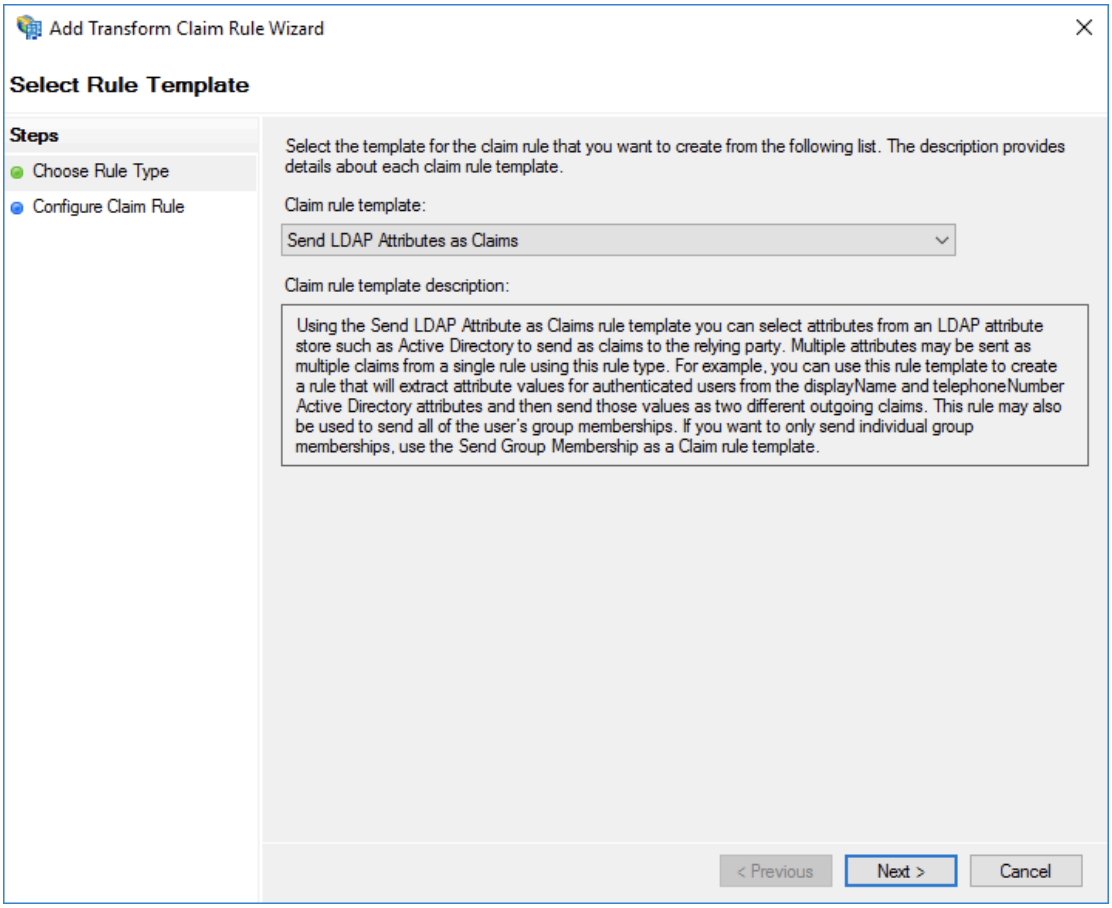
After the configurations are completed, AD FS will send the required `NameID` format to Alibaba Cloud. The following is an example:

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

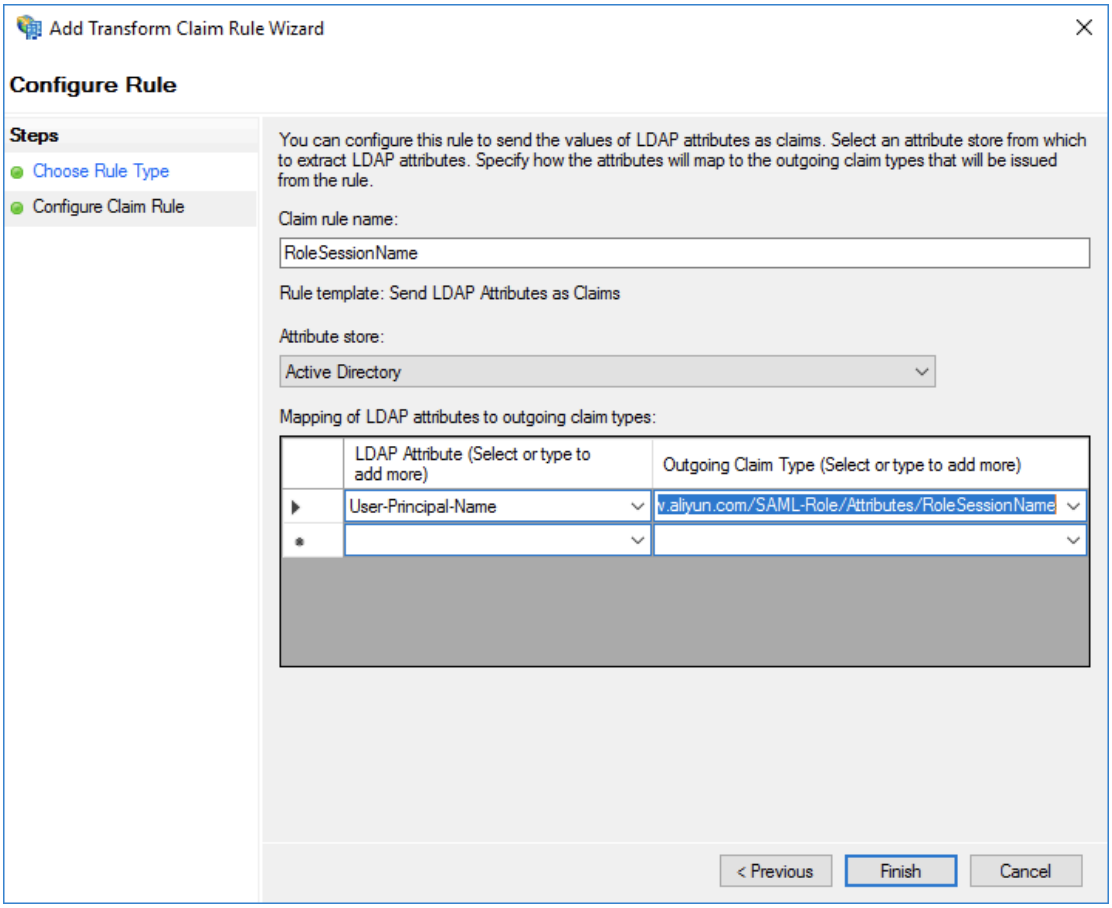
- `RoleSessionName`

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-Role/Attributes/RoleSessionName`



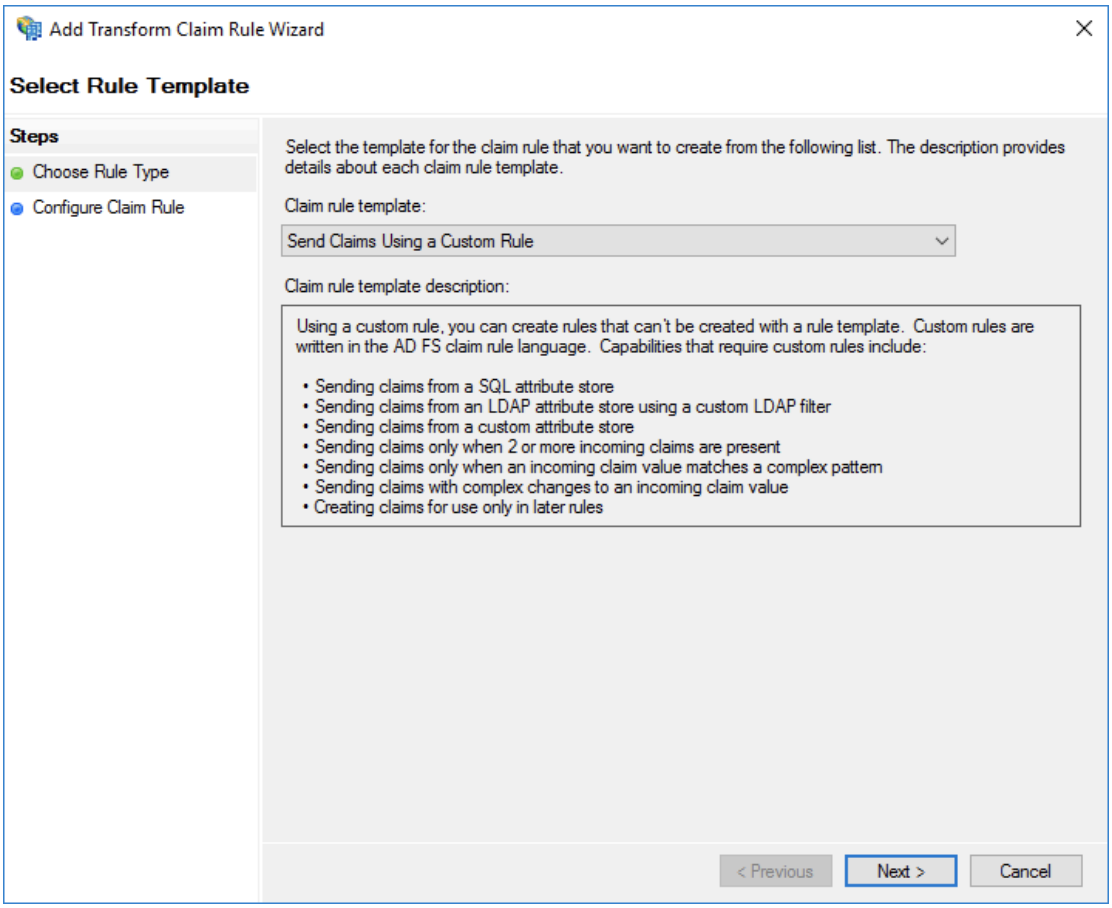
After the configurations are completed, AD FS will send the required `RoleSessio nName` format to Alibaba Cloud. The following is an example:

```
< 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:

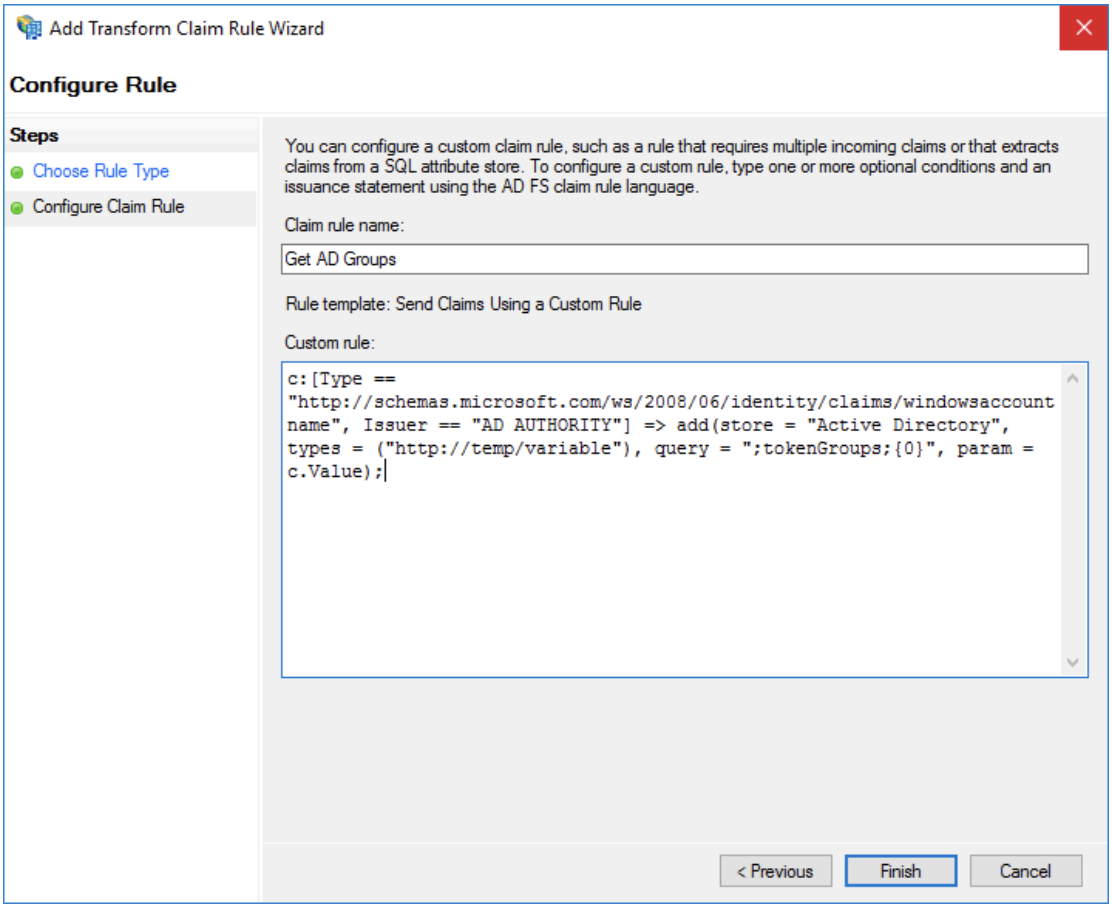
1. Click Add Transform Claim Rule.
2. Select Send Claims Using a Custom Rule from the Claim rule template drop-down list and click Next.



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 / windowsacc  ount
 name ",  Issuer  == " AD   AUTHORITY "] =>  add ( store  = "
 Active   Directory ",
 types  = (" http :// temp / variable "),  query  = ";
 tokenGroup  s ;{ 0 }",  param  =
```

```
c . Value );
```



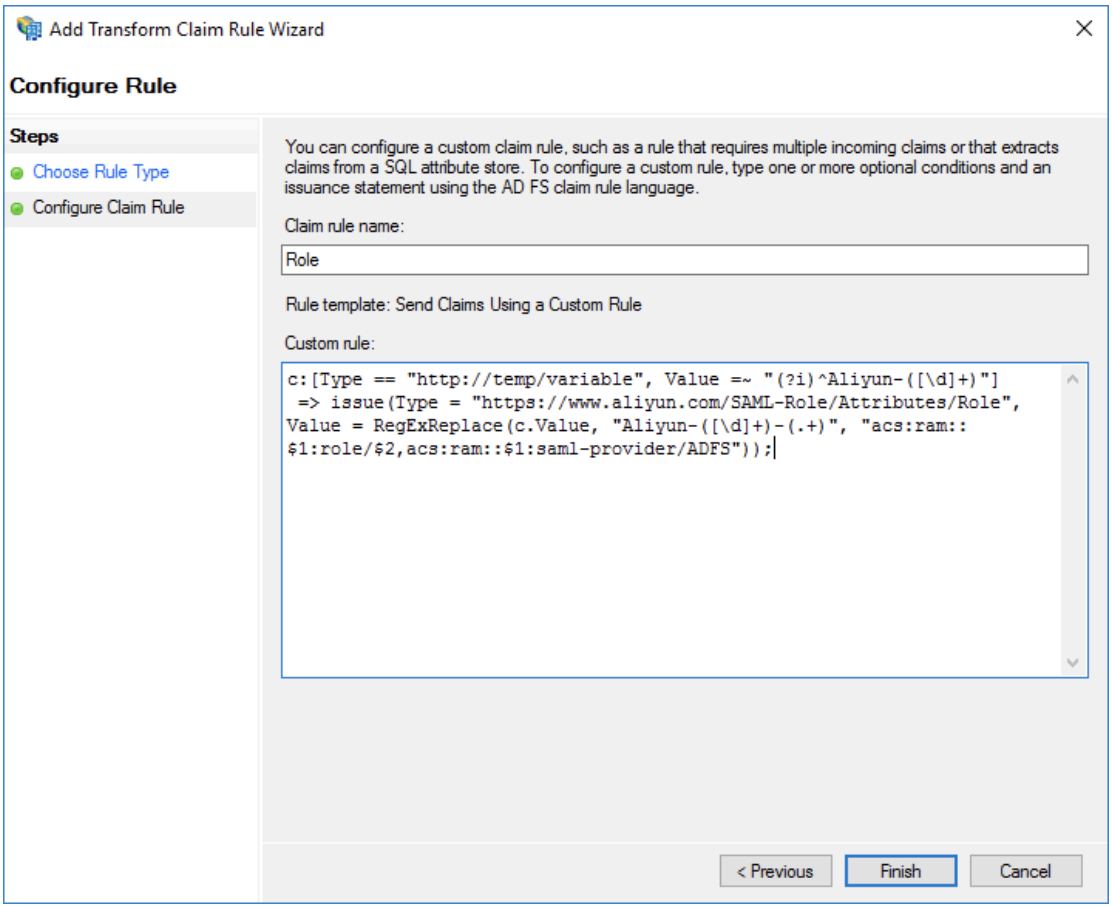
Note:

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
 "));
```



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.

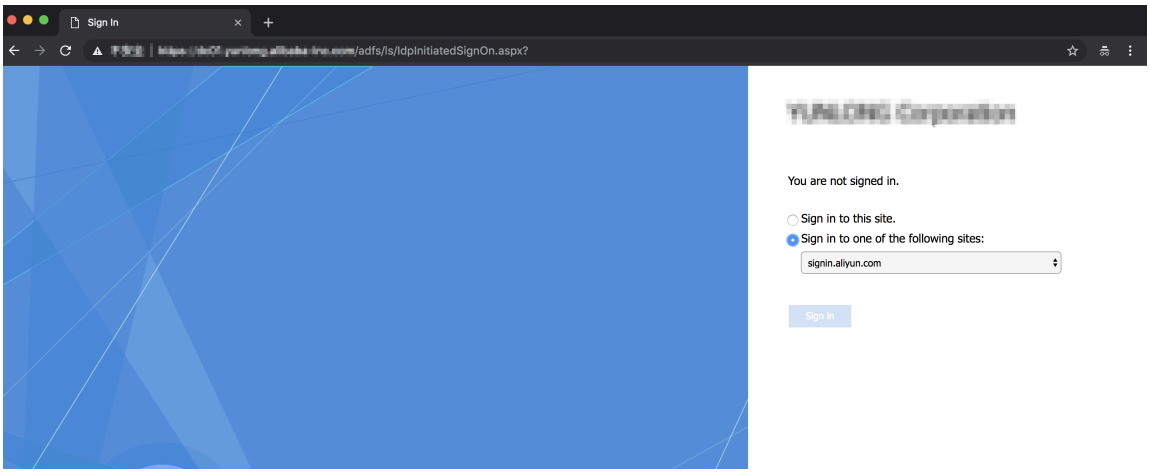
After the configurations are completed, your IdP will return a required SAML assertion to Alibaba Cloud. The following is an example:

```
< 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/IdpInitiatedSignOn.aspx`), select Alibaba Cloud application, and enter the username and password.

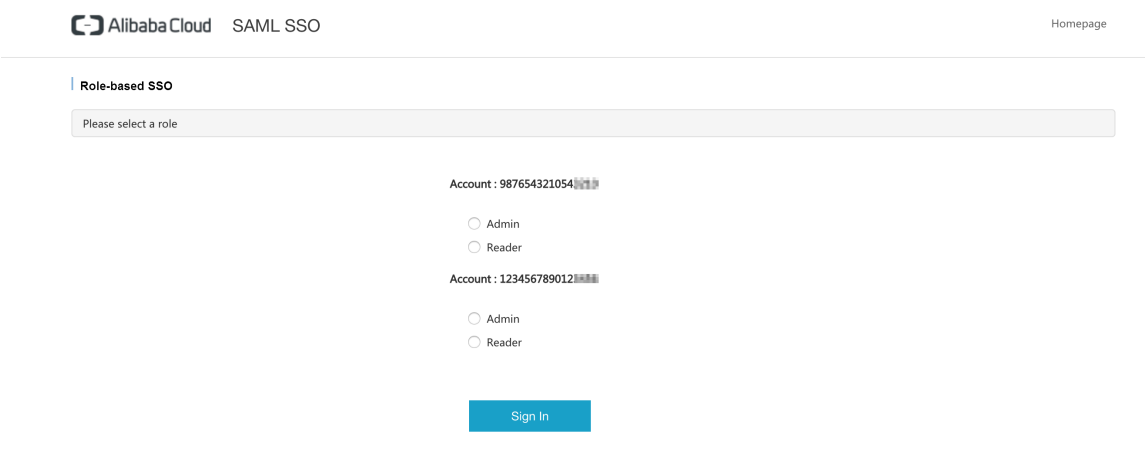
   Note:
   In the preceding URL, <ADFS-server> is the server domain name or IP address of your AD FS. If the URL does not work, run the PowerShell `Set-AdfsProperties -EnableIdpInitiatedSignonPage $True`.

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.

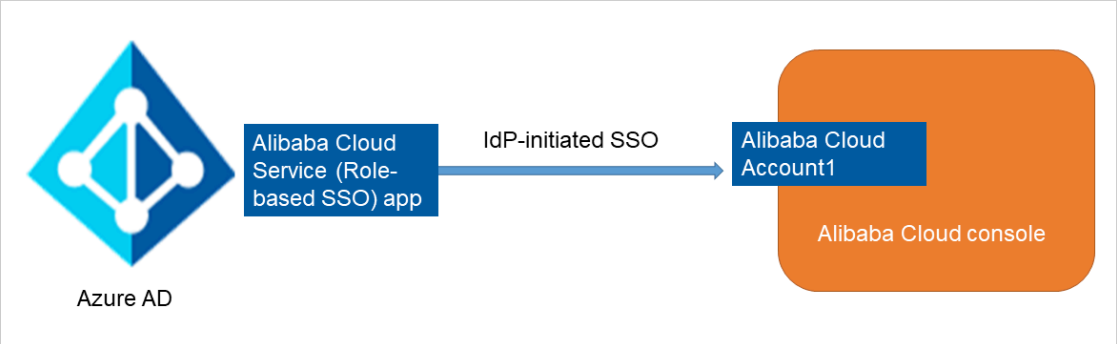


4.7 Implement role-based SSO by using Azure Active Directory

This topic provides an example of how to implement role-based single sign-on (SSO) to Alibaba Cloud from Azure Active Directory (Azure AD). It also helps you to learn about the end-to-end identity SSO process from a cloud identity provider (IdP) to Alibaba Cloud.

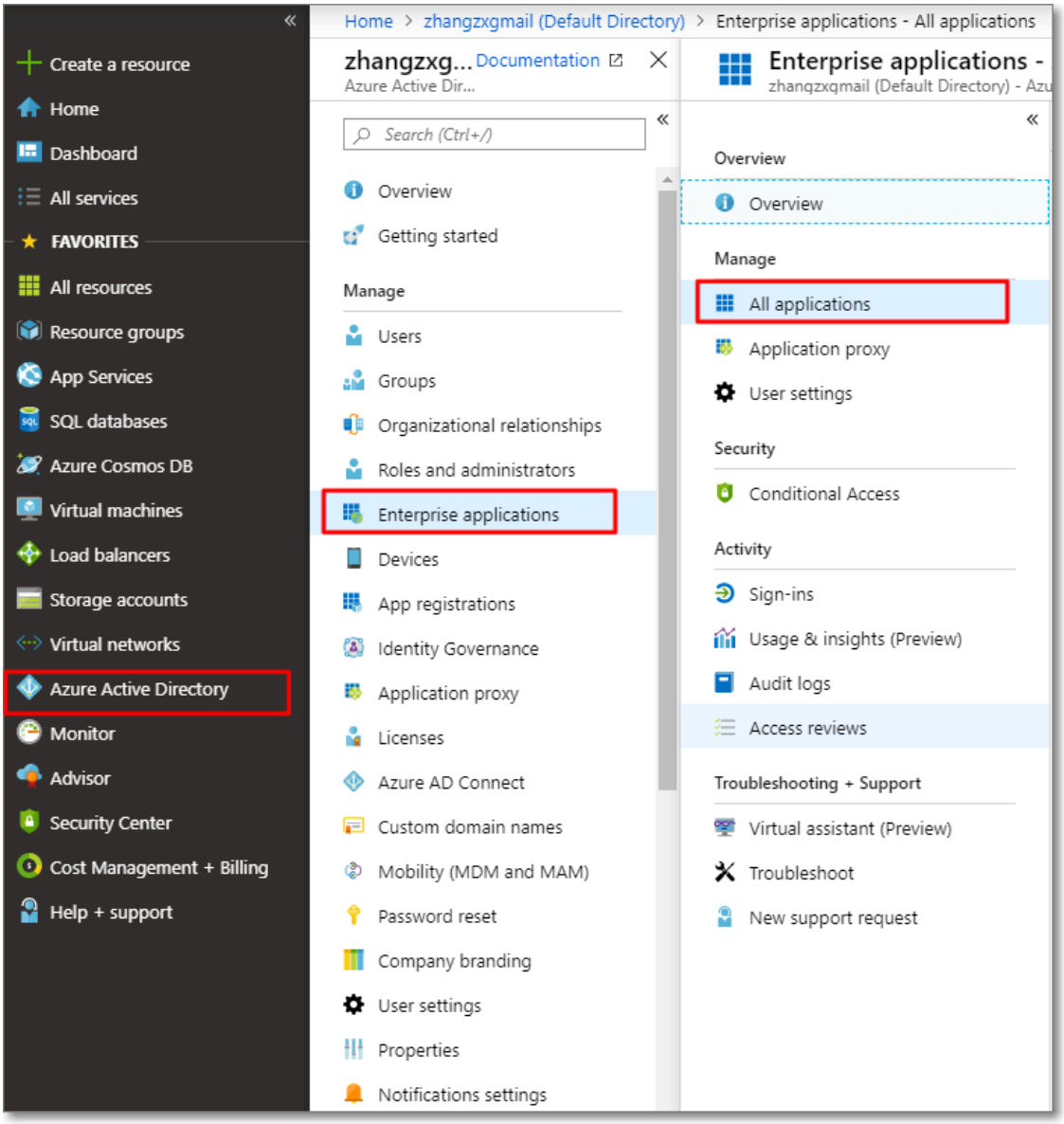
Context

In this example, you have an Alibaba Cloud account (Account1) and an Azure AD user (u2). You use Azure AD to manage your users and configure enterprise applications such as Alibaba Cloud. After implementing role-based SSO, you can better manage your Azure AD users who have access to Alibaba Cloud. You can also enable your users to log on to the Alibaba Cloud console with their Azure AD accounts, and manage your accounts in the Azure portal.

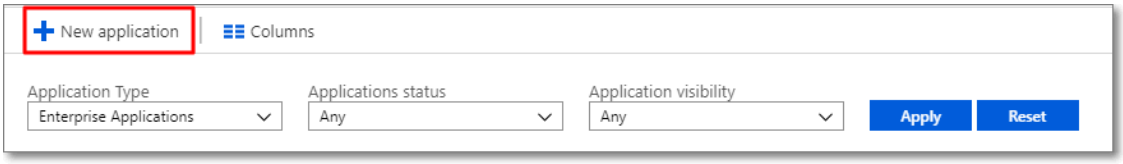


Add Alibaba Cloud role-based SSO from the Azure AD gallery

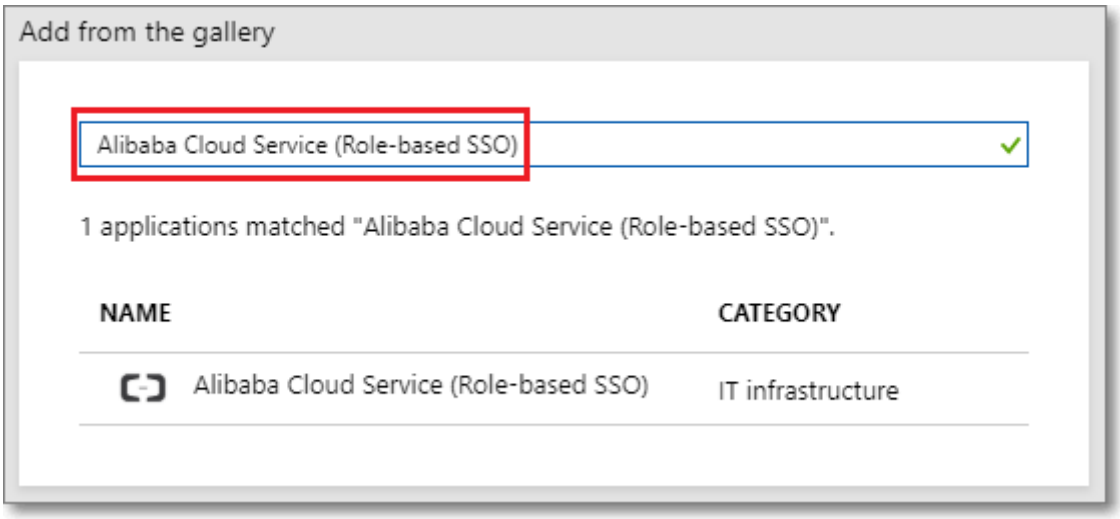
1. Log on to the Azure portal as an administrator.
2. In the left-side navigation pane, choose Azure Active Directory > Enterprise applications > All applications.



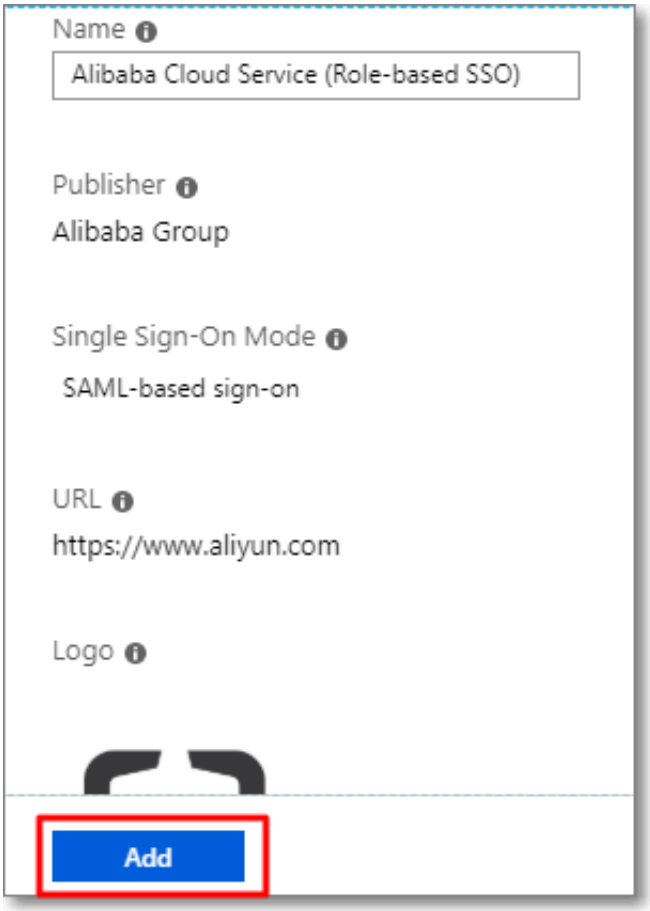
3. Click New application.



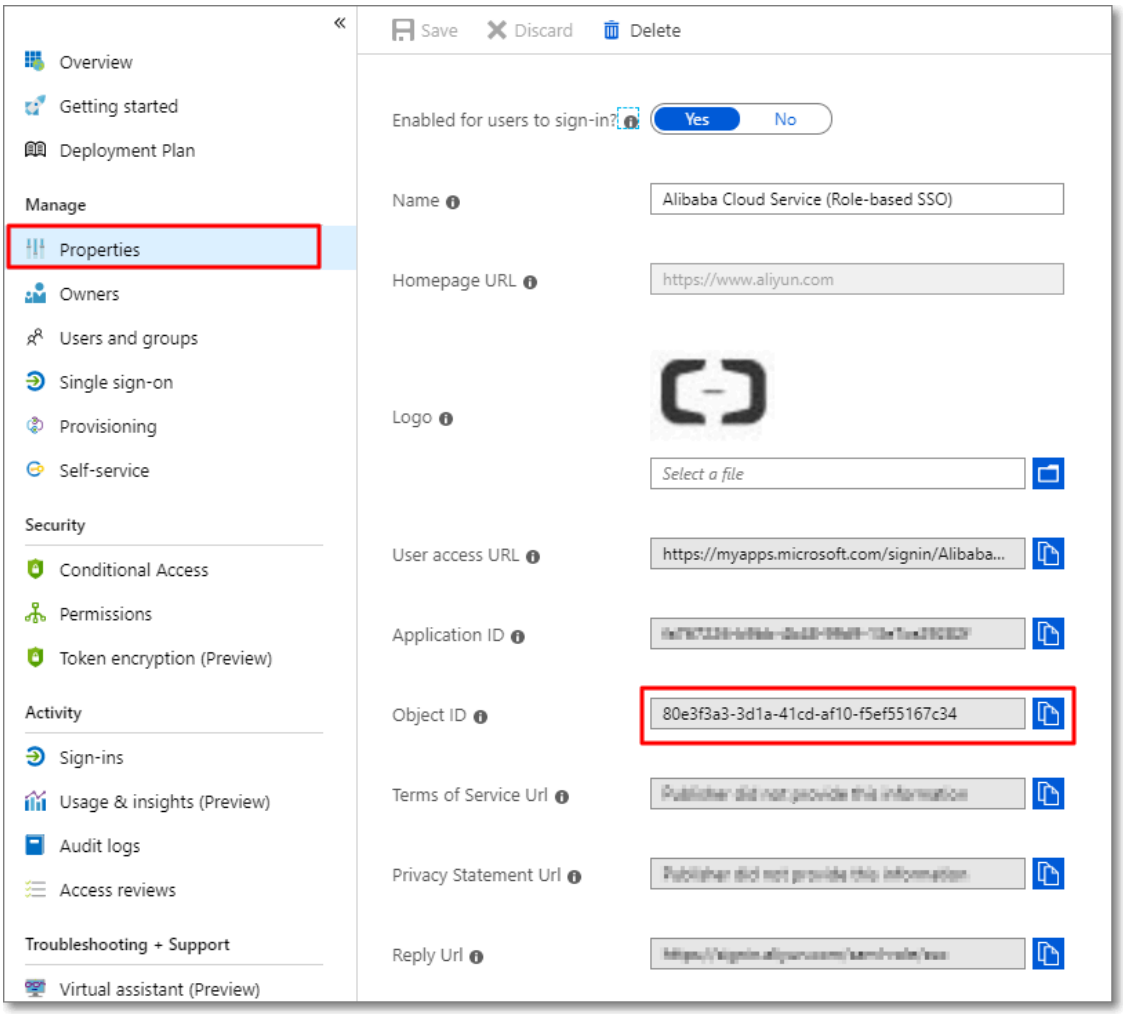
4. In the Add from the gallery section of the Add an application page, enter Alibaba Cloud Service (Role-based SSO) into the textbox and press Enter. Then, select Alibaba Cloud Service (Role-based SSO).



5. On the page that appears, click Add.



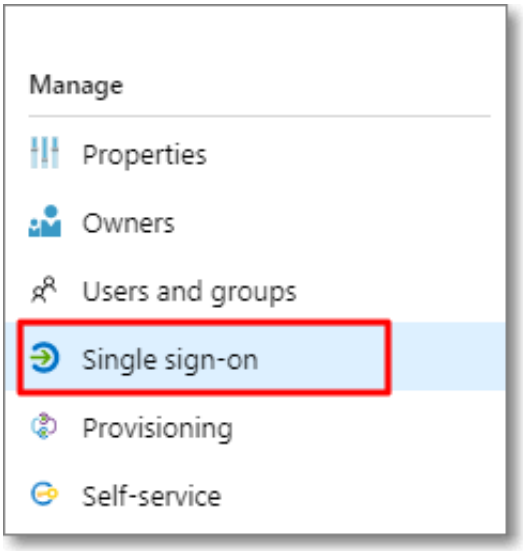
6. On the Alibaba Cloud Service (Role-based SSO) page, click Properties in the left-side navigation pane, and copy and save the object ID for subsequent use.



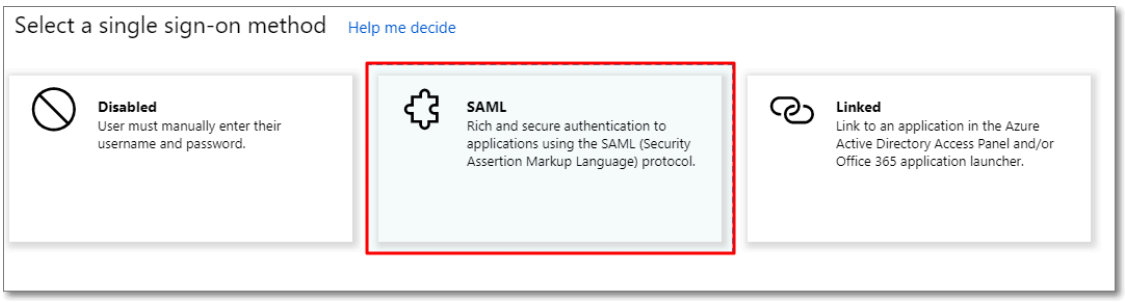
Configure Azure AD SSO

1. Log on to the Azure portal as an administrator.
2. In the left-side navigation pane, choose Azure Active Directory > Enterprise applications > All applications.
3. In the NAME column, click Alibaba Cloud Service (Role-based SSO).

4. In the left-side navigation pane of the page that appears, click Single sign-on.

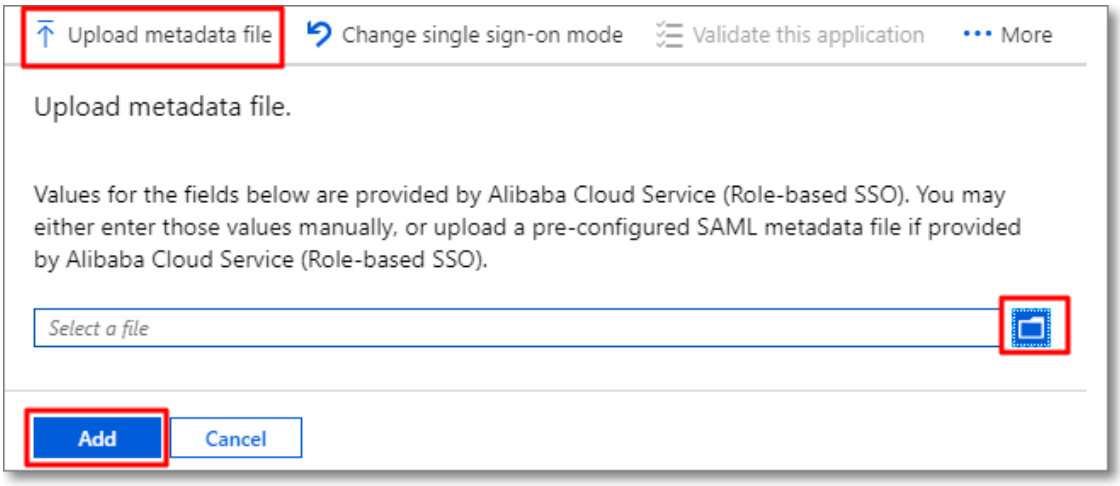


5. In the Select a single sign-on method section, click SAML.



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

   a) In the upper-left corner, click Upload metadata file, select a file, and then click Add.



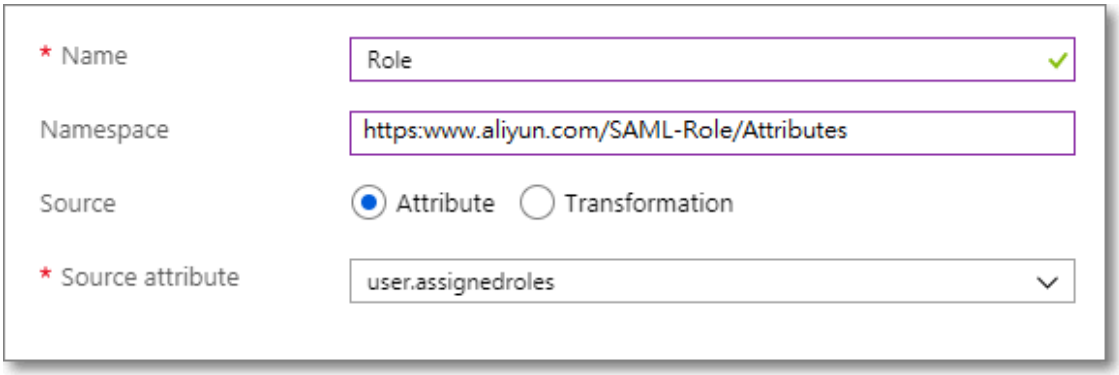
Note:

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

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

c) Click Add new claim, specify the following parameters, and then click Save.

- Specify the Name parameter as `Role`.
- Specify the Namespace parameter as `https://www.aliyun.com/SAML-Role/Attributes`.
- Select Attribute for the Source parameter.
- Select `user.assignedroles` from the Source attribute drop-down list.

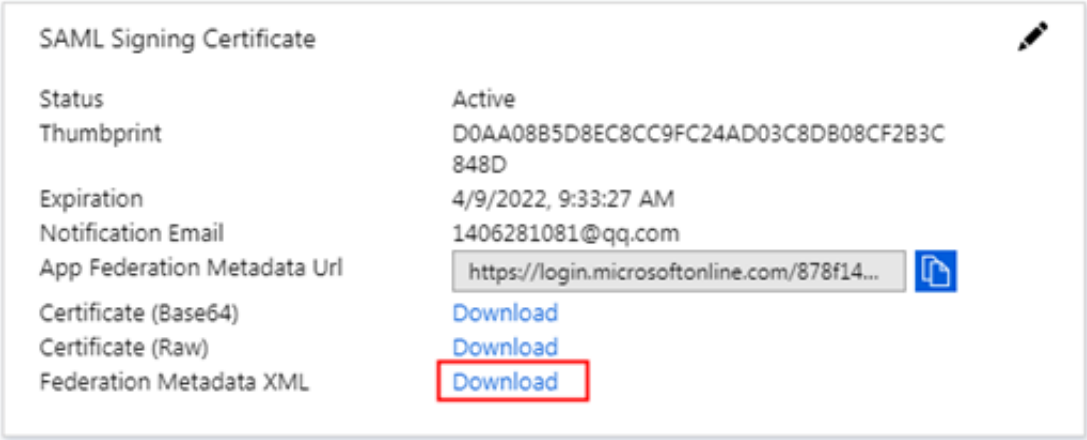


d) Repeat the preceding step to add another claim.

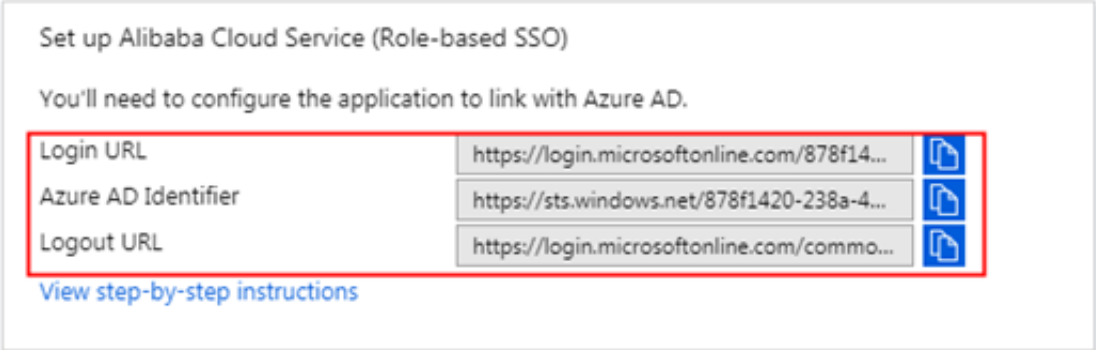
- Specify the Name parameter as `RoleSessionName`.
- Specify the Namespace parameter as `https://www.aliyun.com/SAML-Role/Attributes`.
- Select Attribute for the Source parameter.
- Select `user.userprincipalname` from the Source attribute drop-down list.

e) In the upper-right corner of the User Attributes & Claims page, click the close icon. On the page that appears, in the SAML Signing Certificate section,

click Download next to Federation Metadata XML to download the federation metadata XML for subsequent use.



f) In the Set up Alibaba Cloud Service (Role-based SSO) section, copy and save the Login URL, Azure AD Identifier, and Logout URL for subsequent use.



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, click SSO.
3. On the Role-based SSO page, click Create IdP.
4. On the page that appears, specify the IdP Name parameter as `AAD`, and specify the Note parameter.
5. Click Upload under Metadata File to upload the federation metadata file you downloaded before.

   Note:
   You need to upload the federation metadata file that you have downloaded from the SAML Signing Certificate section in Step 6-e.

6. Click OK.

7. After the IdP is created, click Create RAM Role.
8. Specify the RAM Role Name parameter as `AADrole`, and specify the Note parameter.
9. Select `AAD` from the drop-down list of Select IdP, and click OK.

Note:

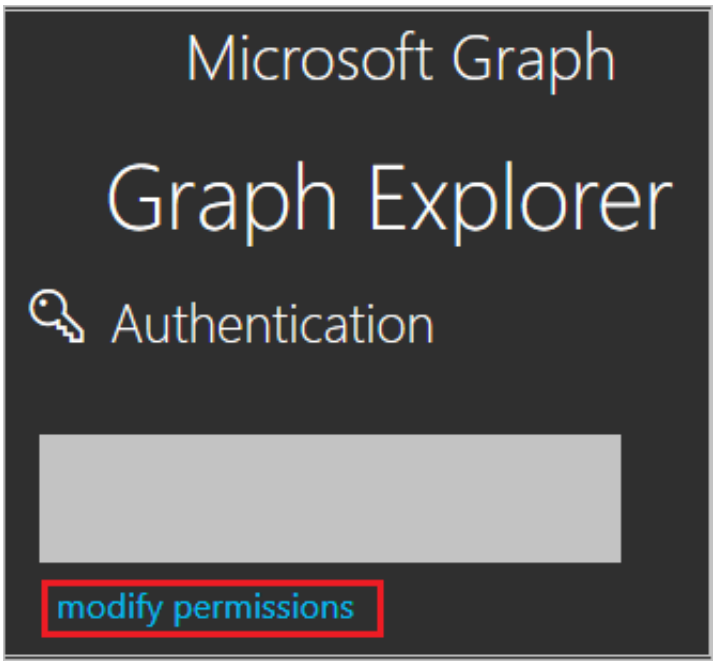
- You can grant permission to the role based on your business needs. For more information, see #unique_39.
- After creating the IdP and the corresponding role, we recommend that you save the ARNs of the IdP and the RAM role for subsequent use. For more information about how to obtain the ARN of the RAM role, see #unique_40.

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

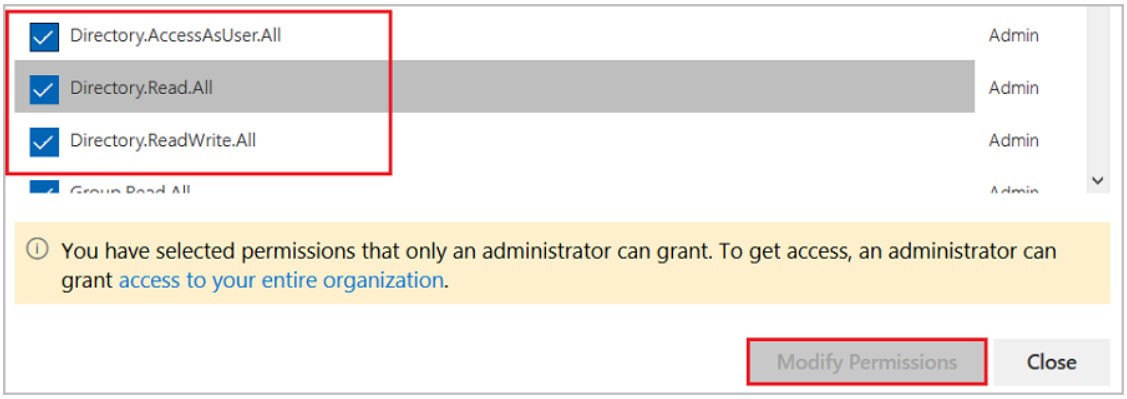
1. To associate the RAM role with the Azure AD user, you must first create a role in Azure AD by following these steps:

   a) Log on to the Azure AD Graph Explorer by using u2.

   b) Click modify permissions to obtain the required permissions.



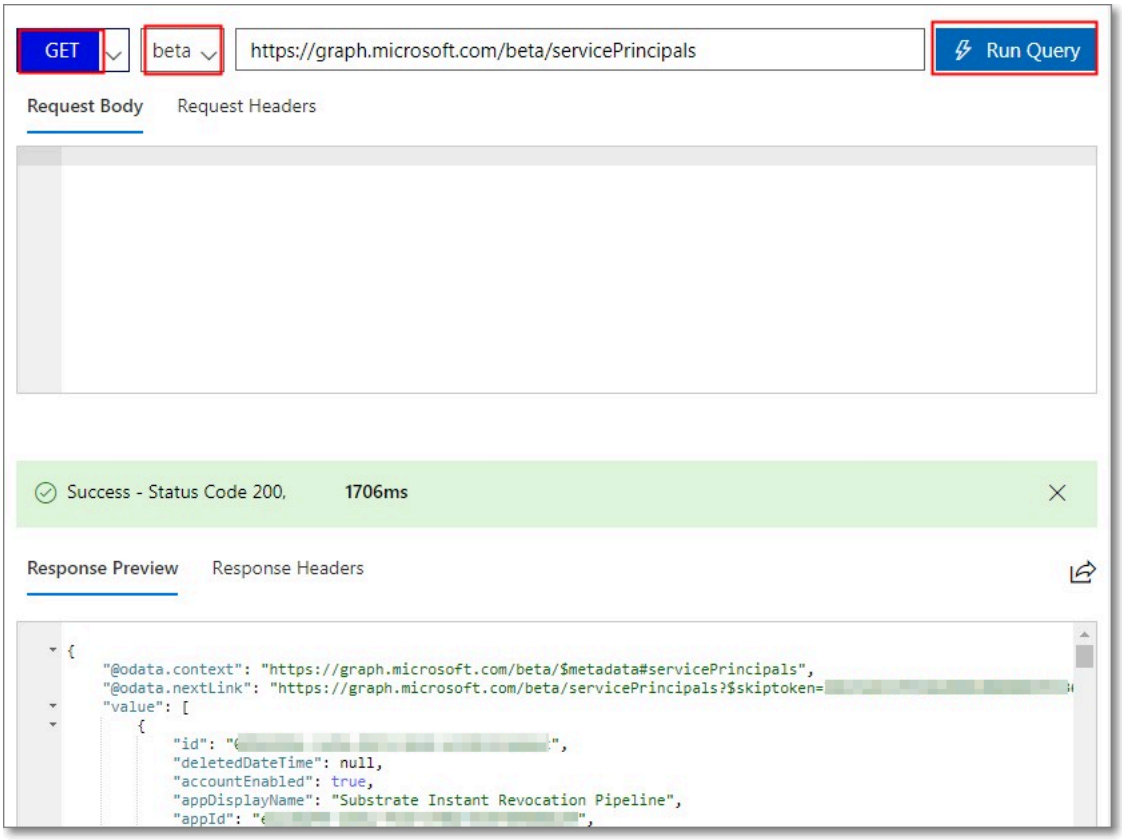
   c) Select the following permissions from the list, and click Modify Permissions.



> **Note:**
> After the permissions are granted, log on to the Graph Explorer again.

   d) On the Graph Explorer page, select GET from the first drop-down list, and select beta from the second drop-down list. Then, enter `https :// graph .`

`microsoft . com / beta / servicePri ncipals` into the textbox next to the drop-down lists, and click Run Query.



Note:

If you are using multiple directories, enter `https :// graph . microsoft . com / beta / contoso . com / servicePri ncipals` into the textbox next to the drop-down lists.

e) On the Response Preview tab, extract the `appRoles` property from the `Service Principal` object for subsequent use.

```
" appRoles ": [
                {
                    " allowedMem berTypes ": [
                        " User "
                    ],
                    " descriptio n ": " msiam_acce ss ",
                    " displayNam e ": " msiam_acce ss ",
                    " id ": " 7dfd756e - 8c27 - 4472 - b2b7 -
38c17fc5 ****",
                    " isEnabled ": true ,
                    " origin ": " Applicatio n ",
                    " value ": null
                }
```

```
            ],
```

Note:

You can find the `appRoles` property by entering `https :// graph . microsoft . com / beta / servicePri ncipals /< objectID >` into the textbox next to the drop-down lists. Note that the value of the `objectID` parameter is the object ID you have copied from the Azure AD Properties page.

f) Go back to the Graph Explorer, select PATCH from the first drop-down list, and select beta from the second drop-down list. Enter `https :// graph . microsoft . com / beta / servicePri ncipals /< objectID >` into the textbox next to the drop-down lists. Copy and paste the following sample script into the Request Body section, edit the script based on your business needs, and click Run Query.

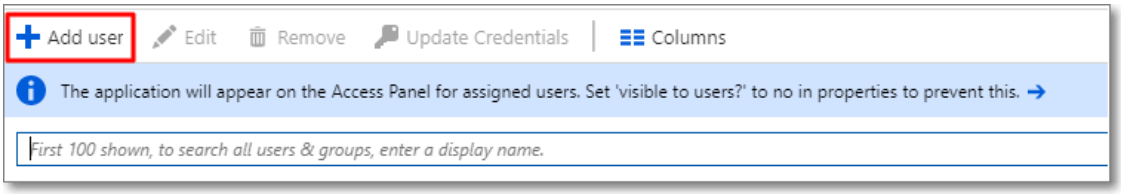
```
{
  " appRoles ": [
    {
      " allowedMem berTypes ":[
        " User "
      ],
      " descriptio n ": " msiam_acce ss ",
      " displayNam e ": " msiam_acce ss ",
      " id ": " 41be2db8 - 48d9 - 4277 - 8e86 - f6d22d35 ****",//
The ID of the RAM role .
      " isEnabled ": true ,
      " origin ": " Applicatio n ",
      " value ": null
    },
    { " allowedMem berTypes ": [
        " User "
    ],
    " descriptio n ": " Admin , AzureADPro d ",
    " displayNam e ": " Admin , AzureADPro d ",
    " id ": " 68adae10 - 8b6b - 47e6 - 9142 - 6476078c ****",//
The ID that is produced by an ID generator in
real time , such as GUID Generator .
    " isEnabled ": true ,
    " origin ": " ServicePri ncipal ",
    " value ": " acs : ram :: 1871250227 22 ****: role / aadrole
, acs : ram :: 1871250227 22 ****: saml - provider / AAD "//
The ARNs of the IdP and the RAM role that you
  created in the RAM console .
    }
  ]
}
```

Note:

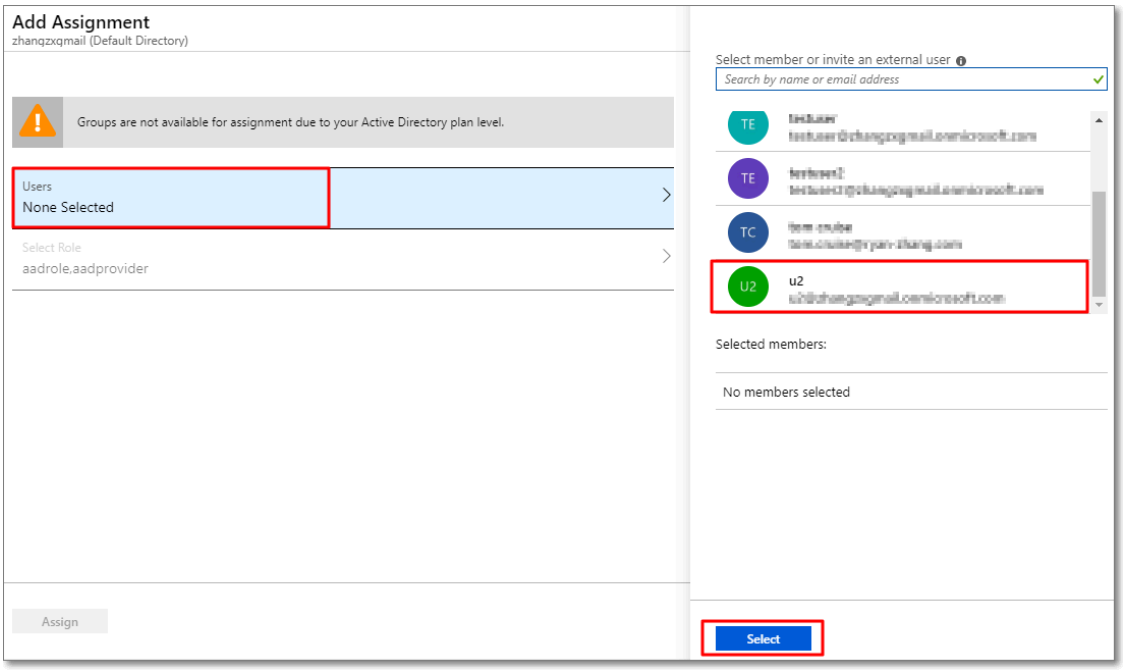
You can add multiple roles based on your business needs. Azure AD will send the ARNs of these roles and their corresponding IdPs as the claim value in

SAML response. However, you can only add new roles after the `msiam_access` part for the patch operation.

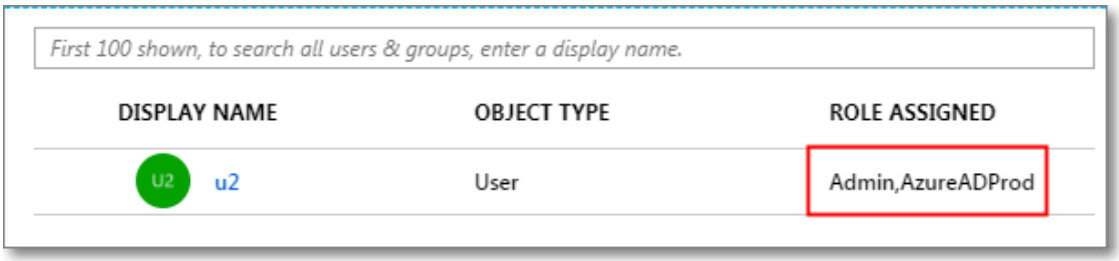
2. Associate the RAM role with the Azure AD user (u2) by following these steps:
   a) Log on to the Azure portal as an administrator.
   b) In the left-side navigation pane, choose Azure Active Directory > Enterprise applications > All applications.
   c) In the NAME column, click Alibaba Cloud Service (Role-based SSO).
   d) In the left-side navigation pane, click Users and groups.
   e) In the upper-left corner, click Add user.



   f) On the page that appears, click Users, select u2 from the user list, and then click Select.



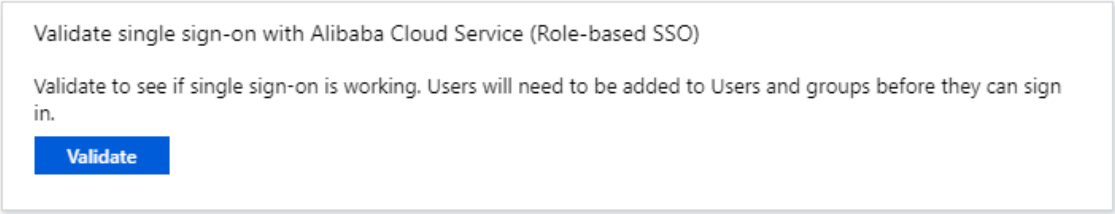
   g) Click Assign.
   h) View the assigned role and test role-based SSO.



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

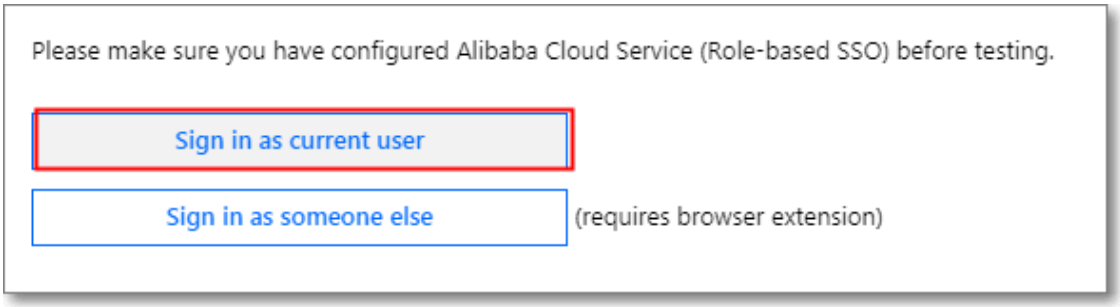
Test role-based SSO

1. Log on to the Azure portal as an administrator.
2. In the left-side navigation pane, choose Azure Active Directory > Enterprise applications > All applications.
3. In the NAME column, click Alibaba Cloud Service (Role-based SSO).
4. In the left-side navigation pane of the page that appears, click Single sign-on.
5. On the page that appears, in the Validate single sign-on with Alibaba Cloud Service (Role-based SSO) section, click Validate.

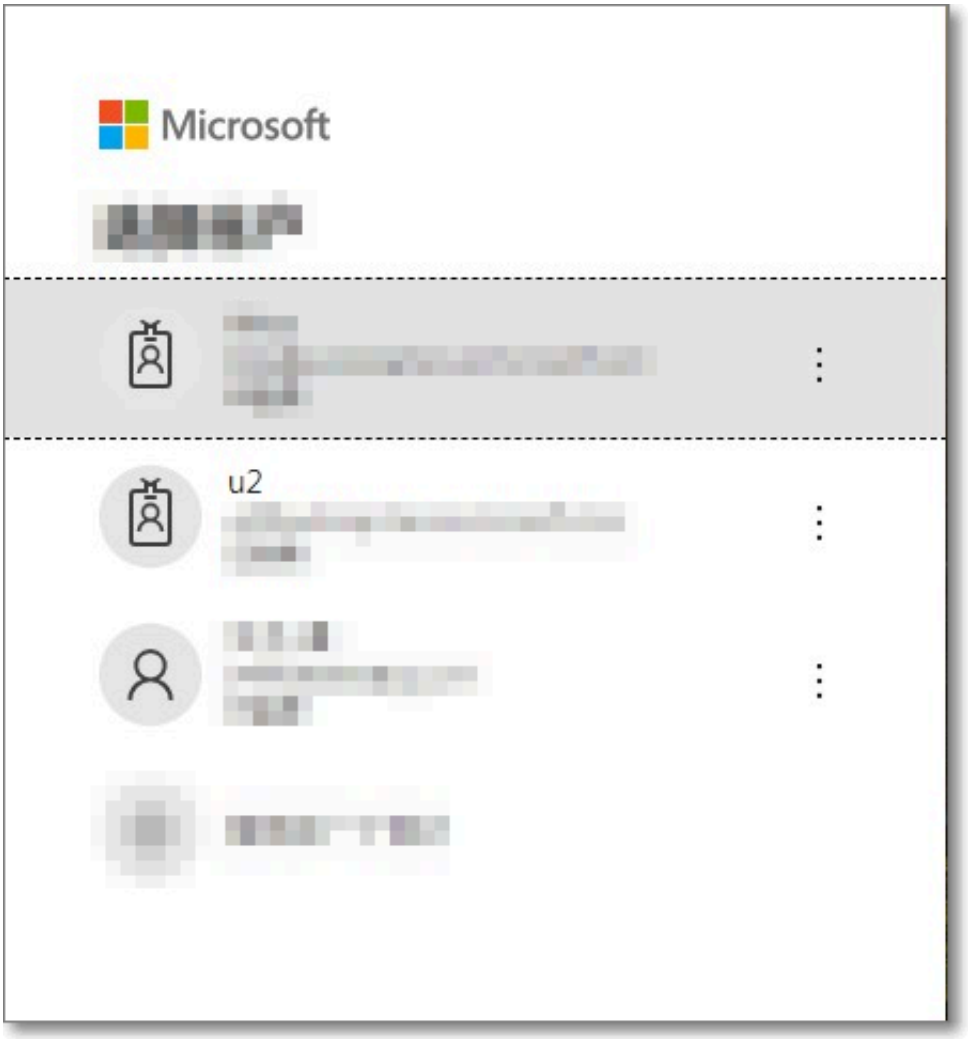


> **Note:**
> Make sure that u2 has been added to a group in Azure AD before you log on to the Azure portal as an administrator.

6. Click Sign in as current user.

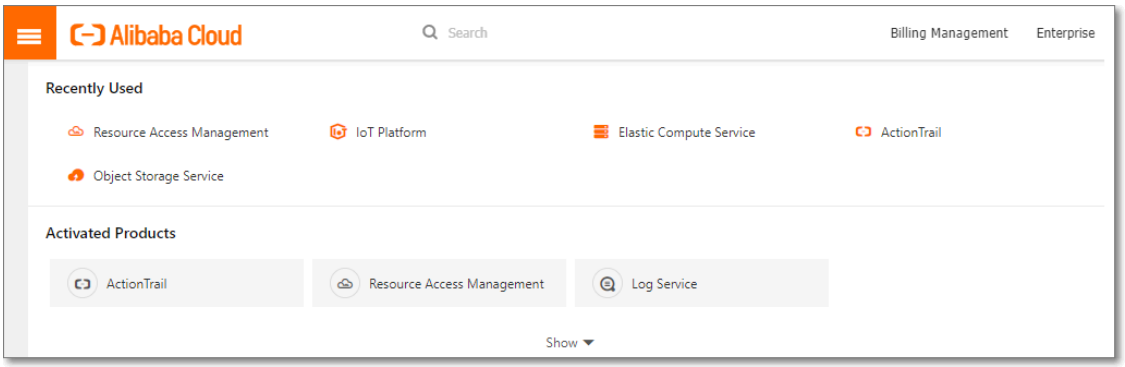


7. On the page for selecting a logon account, select u2.



Result

If the following page appears, it indicates that role-based SSO is successful.



5 Best practices

5.1 Use RAM to maintain security of your Alibaba Cloud resources

This topic describes how to use RAM to apply access and security settings to your Alibaba Cloud resources so that you can better manage access permissions with fine-grained access control.

Prerequisites

An Alibaba Cloud account is created. If not, create one before proceeding. To create an Alibaba Cloud account, click Create a new Alibaba Cloud account.

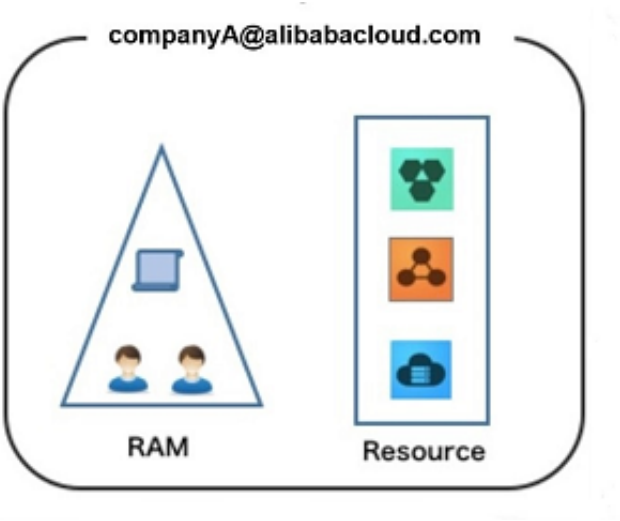
Scenario

When you migrate your business resources to the cloud, the traditional organizati onal structures and previous management methods of your resources may no longer meet your requirements. As a result, the migration of your resources may create higher security management issues as follows:

- The responsibilities of the RAM users are not clear.
- The Alibaba Cloud account owner does not want to share the access key with RAM users due to security risks involved.
- RAM users can access resources by using different methods, which is not unified and may mistakenly cause security risks.
- The resource access permissions of RAM users need to be frequently recalled when the users no longer require these permissions.

Solution

To resolve the preceding issues, you can use RAM to create RAM users and grant resource access permissions to RAM users. Specifically, you can use RAM to separate the access key of your Alibaba Cloud account from RAM users and grant minimum permissions to users as needed to maintain the security of your resources.



Security management solution

- Create independent RAM users.

  An enterprise needs only one Alibaba Cloud account. As a best practice, the Alibaba Cloud account is not used for daily tasks. However, multiple RAM users can be created under the account, and granted the necessary access permissions to resources as needed.

  For more information, see #unique_13.

- Separate console users from API users.

  We recommend that you do not create a logon password for console operations and an access key for API operations for a RAM user at the same time.

  - To allow an application to access cloud resources only through APIs, you only need to create an access key for the application.
  - To allow an employee to operate on cloud resources only through the console, you only need to set a logon password for the employee.

  For more information, see #unique_13.

- Create RAM users and group them.

  If your Alibaba Cloud account has multiple RAM users, you can group RAM users with same responsibilities and grant permissions to the group as needed.

  For more information, see #unique_43.

- Grant the minimum permissions to different RAM user groups.

  You can attach proper system policies to RAM users or user groups as needed. You can also create custom policies for fine-grained permission management. In

this way, by granting the minimum permissions to different RAM users and user groups, you can better manage the RAM users' operations on the cloud resources.

For more information, see #unique_44.

- Configure strong password policies.

  You can configure password policies with custom conventions regarding the minimum length, mandatory characters, and validation period, for RAM users in the RAM console. If a RAM user is allowed to change their logon password, the user must create a strong logon password and rotate the password or access key on a regular basis.

  For more information, see #unique_45.

- Enable an MFA device for your Alibaba Cloud account.

  You can enable a multi-factor authentication (MFA) device for your Alibaba Cloud account to enhance the account security. When you log on to Alibaba Cloud with MFA enabled, the system requires the following two security factors:

  1. Your username and password
  2. Verification code provided by the MFA device

  For more information, see #unique_46.

- Enable SSO for RAM users.

  After Single Sign On (SSO) is enabled, all the internal accounts of your enterprise will be authenticated. Then, users can log on to Alibaba Cloud to access corresponding resources only by using an internal account.

  For more information, see #unique_4.

- Do not share the access key of your Alibaba Cloud account.

  Your Alibaba Cloud account has full control permissions over resources under it, and its access keys have the same permissions as logon passwords. However, access keys are used for programmatic access whereas logon passwords are used to log on to the console. Therefore, to avoid information leaks due to misuse of an access key, we recommend that you do not share or use the access key of your Alibaba Cloud account.

  Instead, create a RAM user and grant this user the relevant permissions.

  For more information, see #unique_47.

- Specify operation conditions to enhance security.

  You can specify the operational conditions that a RAM user must meet before they can use your cloud resources. For example, you can specify that the RAM user must use a secure channel (such as SSL), use a specified source IP address, or operate within a specified period of time.

  For more information, see #unique_48.

- Manage permissions of your cloud resources.

  By default, all your resources are under your Alibaba Cloud account. A RAM user can use the resources but do not own the resources. This allows you to easily manage the instances or data created by RAM users.

  - For an existing RAM user that you no long require, you can remove all of its corresponding permissions by simply removing the RAM user account.
  - For a RAM user that requires a permission, you need to first create the RAM user , set the logon password or access key for it, and then grant the RAM user the relevant permissions as needed.

  For more information, see #unique_49.

- Use STS to grant temporary permissions to RAM users.

  The Security Token Service (STS) is an extended authorization service of RAM. You can use STS to grant temporary permissions to RAM users and specify the permission and automatic expiration time of the tokens as needed.

  For more information, see #unique_50

Result

After migrating your services to the cloud, you can use the preceding solutions to ensure you manage your cloud-based resources effectively and keep your Alibaba Cloud account and all business assets secure.

What to do next

You can use RAM to categorize your O&M requirements and assign tasks to different engineers as needed. For more information, see #unique_51.