ALIBABA CLOUD

Alibaba Cloud

访问控制

单点登录管理（SSO）

文档版本：20220628

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.SSO概览 06
2.SSO方式的适用场景 08
3.用户SSO 09
3.1. 用户SSO概览 09
3.2. 进行用户SSO时阿里云SP的SAML配置 10
3.3. 进行用户SSO时企业IdP的SAML配置 11
3.4. 用户SSO的SAML响应 11
3.5. 使用AD FS进行用户SSO的示例 14
3.6. 使用Okta进行用户SSO的示例 19
3.7. 使用Azure AD进行用户SSO的示例 23
4.角色SSO 27
4.1. 基于SAML的角色SSO 27
4.1.1. SAML角色SSO概览 27
4.1.2. SAML身份提供商 28
4.1.2.1. 创建SAML身份提供商 29
4.1.2.2. 查看SAML身份提供商基本信息 29
4.1.2.3. 修改SAML身份提供商基本信息 29
4.1.2.4. 删除SAML身份提供商 30
4.1.3. 进行角色SSO时阿里云SP的SAML配置 30
4.1.4. 进行角色SSO时企业IdP的SAML配置 30
4.1.5. 角色SSO的SAML响应 31
4.1.6. 使用AD FS进行角色SSO的示例 35
4.1.7. 使用Okta进行角色SSO的示例 41
4.1.8. 使用Azure AD进行角色SSO的示例 48
4.1.9. 使用OneLogin进行角色SSO的示例 52
4.2. 基于OIDC的角色SSO 55

4.2.1. OIDC角色SSO概览 55
4.2.2. 管理OIDC身份提供商 57
4.2.3. 使用OIDC进行角色SSO的示例 58

1.SSO概览

阿里云支持基于SAML 2.0和OIDC的SSO（Single Sign On，单点登录），也称为身份联合登录。本文为您介绍企业如何使用自有的身份系统实现与阿里云的SSO。

SSO基本概念

概念	说明
身份提供商（IdP）	一个包含有关外部身份提供商元数据的RAM实体，身份提供商可以提供身份管理服务。 • 企业本地IdP：Microsoft Active Directory Federation Service （AD FS）、Shibboleth等。 • Cloud IdP：Azure AD、Google G Suite、Okta、OneLogin等。
服务提供商（SP）	利用IdP的身份管理功能，为用户提供具体服务的应用，SP会使用IdP提供的用户信息。一些非SAML协议的身份系统（例如：OpenID Connect），也把服务提供商称作IdP的信赖方。
安全断言标记语言（SAML 2.0）	实现企业级用户身份认证的标准协议，它是SP和IdP之间实现沟通的技术实现方式之一。SAML 2.0已经是目前实现企业级SSO的一种事实标准。
SAML断言（SAML assertion）	SAML协议中用来描述认证请求和认证响应的核心元素。例如：用户的具体属性就包含在认证响应的断言里。
信赖（Trust）	建立在SP和IdP之间的互信机制，通常由公钥和私钥来实现。SP通过可信的方式获取IdP的SAML元数据，元数据中包含IdP签发SAML断言的签名验证公钥，SP则使用公钥来验证断言的完整性。
OIDC	OIDC（OpenID Connect）是建立在OAuth 2.0基础上的一个认证协议。OAuth是授权协议，而OIDC在OAuth协议上构建了一层身份层，除了OAuth提供的授权能力，它还允许客户端能够验证终端用户的身份，以及通过OIDC协议的API（HTTP RESTful形式）获取用户的基本信息。
OIDC令牌	OIDC可以给应用签发代表登录用户的身份令牌，即OIDC令牌（OIDC Token）。OIDC令牌用于获取登录用户的基本信息。
客户端ID	您的应用在外部IdP注册的时候，会生成一个客户端ID（Client ID）。当您从外部IdP申请签发OIDC令牌时必须使用该客户端ID，签发出来的OIDC令牌也会通过 `aud` 字段携带该客户端ID。在创建OIDC身份提供商时配置该客户端ID，然后在使用OIDC令牌换取STS Token时，阿里云会校验OIDC令牌中 `aud` 字段所携带的客户端ID与OIDC身份提供商中配置的客户端ID是否一致。只有一致时，才允许扮演角色。
验证指纹	为了防止颁发者URL被恶意劫持或篡改，您需要配置外部IdP的HTTPS CA证书生成的验证指纹。阿里云会辅助您自动计算该验证指纹，但是建议您在本地自己计算一次（例如：使用OpenSSL计算指纹），与阿里云计算的指纹进行对比。如果对比发现不同，则说明该颁发者URL可能已经受到攻击，请您务必再次确认，并填写正确的指纹。
颁发者URL	颁发者URL由外部IdP提供，对应OIDC Token中的 `iss` 字段值。颁发者URL必须以 `https` 开头，符合标准URL格式，但不允许带有query参数（以 `?` 标识）、fragment片段（以 `#` 标识）和登录信息（以 `@` 标识）。

概念	说明
临时身份凭证	STS（Security Token Service）是阿里云提供的一种临时访问权限管理服务，通过STS获取可以自定义时效和访问权限的临时身份凭证（STS Token）。

SSO方式

阿里云提供以下两种SSO方式：

- 用户SSO

  阿里云通过IdP颁发的SAML断言确定企业用户与阿里云RAM用户的对应关系 。企业用户登录后，使用该RAM用户访问阿里云资源。更多信息，请参见用户SSO概览。

- 角色SSO

  支持基于SAML 2.0和OIDC的两种角色SSO：

  - SAML角色SSO：阿里云通过IdP颁发的SAML断言确定企业用户在阿里云上可以使用的RAM角色。企业用户登录后，使用SAML断言中指定的RAM角色访问阿里云资源。请参见SAML角色SSO概览。
  - OIDC角色SSO：企业用户通过IdP签发的OIDC令牌（OIDC Token），调用阿里云API扮演指定角色并换取角色临时身份凭证（STS Token），然后使用STS Token安全地访问阿里云资源。更多信息，请参见OIDC角色SSO概览。

SSO方式比较

SSO方式	SP发起的SSO	IdP发起的SSO	使用RAM用户账号和密码登录	一次性配置IdP关联多个阿里云账号	多个IdP
用户SSO	支持	支持	不支持	不支持	不支持
角色SSO	不支持	支持	支持	支持	支持

> **说明** 关于用户SSO与角色SSO的更多比较，请参见SSO方式的适用场景。

2.SSO方式的适用场景

阿里云目前支持两种SSO方式：角色SSO和用户SSO。本文为您介绍这两种方式的适用场景和选择依据，帮助您根据整体业务需求选择合适的SSO方式。

角色SSO

角色SSO适用于以下场景：

- 出于管理成本考虑，您不希望在云端创建和管理用户，从而避免用户同步带来的工作量。
- 您希望在使用SSO的同时，仍然保留一部分云上本地用户，可以在阿里云直接登录。云上本地用户的用途可以是新功能测试、网络或企业IdP出现问题时的备用登录方式等。
- 您希望根据用户在本地IdP中加入的组或者用户的某个特殊属性，来区分云上拥有的权限。当进行权限调整时，只需要在本地进行分组或属性的更改。
- 您拥有多个阿里云账号但使用统一的企业IdP，希望在企业IdP配置一次，就可以实现到多个阿里云账号的SSO。
- 您的各个分支机构存在多个IdP，都需要访问同一个阿里云账号，您需要在一个阿里云账号内配置多个IdP进行SSO。
- 除了控制台，您也希望使用程序访问的方式来进行SSO。

用户SSO

用户SSO适用于以下场景：

- 您希望从阿里云的登录页面开始发起登录，而非直接访问您IdP的登录页面。
- 您需要使用的云产品中有部分暂时不支持角色访问。支持角色访问（即通过STS访问）的云产品请参见支持STS的云服务。
- 您的IdP不支持复杂的自定义属性配置。
- 您没有上述需要使用角色SSO的业务需求，而又希望尽量简化IdP配置。

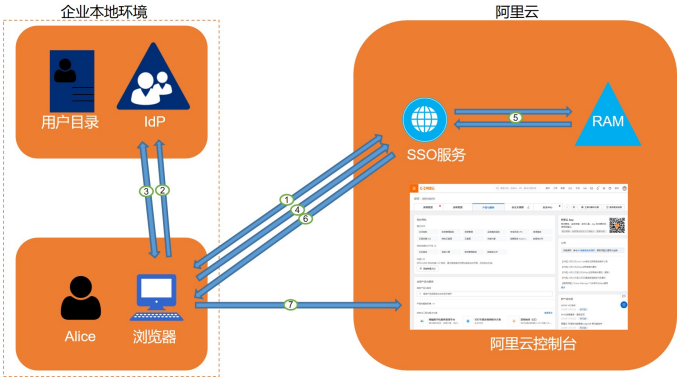
3.用户SSO

3.1. 用户SSO概览

阿里云与企业进行用户SSO时，阿里云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过用户SSO，企业员工在登录后，将以RAM用户访问阿里云。

基本流程

当管理员在完成用户SSO的相关配置后，企业员工Alice可以通过如下图所示的方法登录到阿里云。



1. Alice使用浏览器登录阿里云，阿里云将SAML认证请求返回给浏览器。
2. 浏览器向IdP转发SAML认证请求。
3. IdP提示Alice登录，并在Alice登录成功后生成SAML响应返回给浏览器。
4. 浏览器将SAML响应转发给SSO服务。
5. SSO服务通过SAML互信配置，验证SAML响应的数字签名来判断SAML断言的真伪，并通过SAML断言的 `NameID` 元素值，匹配到对应阿里云账号中的RAM用户。
6. SSO服务向浏览器返回控制台的URL。
7. 浏览器重定向到阿里云控制台。

> **说明** 在第步中，企业员工从阿里云发起登录并不是必须的。企业员工也可以在企业自有IdP的登录页直接单击登录到阿里云的链接，向企业IdP发出登录到阿里云的SAML认证请求。

配置步骤

为了建立阿里云与企业IdP之间的互信关系，需要进行阿里云作为SP的SAML配置和企业IdP的SAML配置，配置完成后才能进行用户SSO。

1. 为了建立阿里云对企业IdP的信任，需要将企业IdP配置到阿里云。

   更多信息，请参见进行用户SSO时阿里云SP的SAML配置。

2. 为了建立企业IdP对阿里云的信任，需要在企业IdP中配置阿里云为可信SAML SP并进行SAML断言属性的配置。

   更多信息，请参见进行用户SSO时企业IdP的SAML配置。

3. 企业IdP和阿里云均配置完成后，企业需要使用SDK、CLI或登录到RAM控制台创建与企业IdP匹配的RAM用户。

   更多信息，请参见创建RAM用户。

配置示例

以下为您提供了常见的企业IdP（例如：AD FS、Okta和Azure AD）与阿里云进行用户SSO的配置示例：

- 使用AD FS进行用户SSO的示例
- 使用Okta进行用户SSO的示例
- 使用Azure AD进行用户SSO的示例

3.2. 进行用户SSO时阿里云SP的SAML配置

本文介绍通过基于SAML 2.0的用户SSO，配置相应元数据来建立阿里云对企业身份提供商（IdP）的信任，实现企业IdP通过用户SSO登录阿里云。

背景信息

设置默认域名、域别名或辅助域名可以简化SAML SSO的配置流程。关于如何设置阿里云账号的默认域名或域别名，请参见查看和修改默认域名和创建并验证域别名。

操作步骤

1. 阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**用户SSO**页签下，可查看当前**SSO登录设置**相关信息。
4. 单击**编辑**，可以配置**SSO登录设置**相关信息，包括选择SSO功能状态、上传元数据文档和设置辅助域名。
   - **SSO功能状态**：可以选择**开启**或**关闭**。

     > **说明** 该功能只对阿里云账号下的所有RAM用户生效，不会影响阿里云账号的登录。

     - 此功能默认为**关闭**，此时RAM用户可以使用密码登录，所有SSO设置不生效。
     - 如果选择**开启**此功能，此时RAM用户密码登录方式将会被关闭，统一跳转到企业IdP登录服务进行身份认证。如果再次关闭，用户密码登录方式自动恢复。
   - **元数据文档**：单击**上传文件**，上传企业IdP提供的元数据文档。

     > **说明** 元数据文档由企业IdP提供，一般为XML格式，包含IdP的登录服务地址以及X.509公钥证书（用于验证IdP所颁发的SAML断言的有效性）。
   - **辅助域名**（可选）：开启辅助域名开关，可以设置一个辅助域名。
     - 如果设置了辅助域名，SAML断言中的`NameID`元素将可以使用此辅助域名作为后缀。
     - 如果没有设置辅助域名，SAML断言中的`NameID`元素将只能使用当前账号的默认域名或域别名作为后缀。

     关于`NameID`元素的取值，请参见用户SSO的SAML响应。

     > **说明** 如果您同时设置了域别名和辅助域名，辅助域名将不会生效。此时，`NameID`元素只能使用域别名或默认域名作为后缀。
5. 单击**确定**。

后续步骤

完成SAML配置后，选择以下一种方法创建与企业IdP相匹配的RAM用户：

- 登录RAM控制台手动创建与企业IdP匹配的RAM用户，详情请参见创建RAM用户。
- 使用RAM SDK编写程序或阿里云CLI来创建RAM用户，详情请参见CreateUser。

3.3. 进行用户SSO时企业IdP的SAML配置

本文主要介绍企业在使用用户SSO时，如何在企业身份提供商（IdP）中配置阿里云为可信SAML服务提供商（SP）。

操作步骤

1. 从阿里云获取SAML服务提供商元数据URL。
   i. 使用阿里云账号登录RAM控制台。
   ii. 在左侧导航栏，单击**SSO管理**。
   iii. 在**SSO管理**页面，单击**用户SSO**页签。
   iv. 在**SSO登录设置**区域，查看当前阿里云账号的**SAML服务提供商元数据URL**。
2. 在企业IdP中创建一个SAML SP，并根据实际情况选择下面任意一种方式配置阿里云为信赖方。
   - 直接使用步骤所述的阿里云元数据URL进行配置。
   - 如果您的IdP不支持URL配置，您可以通过步骤所述URL下载元数据文件并上传至您的IdP。
   - 如果您的IdP不支持元数据文件上传，则需要手动配置以下参数：
     - `Entity ID`：下载的元数据XML中，`md:EntityDescriptor`元素的`entityID`属性值。
     - `ACS URL`：下载的元数据XML中，`md:AssertionConsumerService`元素的`Location`属性值。
     - `RelayState`（可选）：如果您的IdP支持设置`RelayState`参数，您可以将其配置成SSO登录成功后希望跳转到的页面URL。如果不进行配置，SSO登录成功后，将会跳转到阿里云控制台首页。

       > **说明** 出于安全原因，您只能填写阿里巴巴旗下的域名URL作为`RelayState`的值，例如：*.aliyun.com、*.hichina.com、*.yunos.com、*.taobao.com、*.tmall.com、*.alibabacloud.com、*.alipay.com。

后续步骤

在企业IdP中配置阿里云为可信SAML SP后，需要在企业IdP中配置SAML断言属性。更多信息，请参见用户SSO的SAML响应。

3.4. 用户SSO的SAML响应

本文为您介绍进行用户SSO时SAML响应中必须包含的元素，尤其是SAML断言中的元素。

背景信息

在基于SAML 2.0的SSO流程中，当企业用户在IdP登录后，IdP将根据SAML 2.0 HTTP-POST绑定的要求生成包含SAML断言的认证响应，并由浏览器（或程序）自动转发给阿里云。这个SAML断言会被用来确认用户登录状态并从中解析出登录的主体。因此，断言中必须包含阿里云要求的元素，否则登录用户的身份将无法被确认，导致SSO失败。

SAML响应

请确保您的IdP向阿里云发出符合如下要求的SAML响应，每一个元素都必须要有，否则SSO将会失败。

```
<saml2p:Response>
    <saml2:Issuer>...</saml2:Issuer>
    <saml2p:Status>
        ...
    </saml2p:Status>
    <saml2:Assertion>
        <saml2:Issuer>...</saml2:Issuer>
        <ds:Signature>
            ...
        </ds:Signature>
        <saml2:Subject>
            <saml2:NameID>${NameID}</saml2:NameID>
            <saml2:SubjectConfirmation>
                ...
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions>
            <saml2:AudienceRestriction>
                <saml2:Audience>${Audience}</saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement>
            ...
        </saml2:AuthnStatement>
    </saml2:Assertion>
</saml2p:Response>
```

SAML断言中的元素说明

- **SAML 2.0协议的通用元素**

元素	说明
`Issuer`	`Issuer` 的值必须与您在阿里云用户SSO设置中上传的元数据文件中的 `EntityID` 匹配。
`Signature`	阿里云要求SAML断言必须被签名以确保没有篡改， `Signature` 及其包含的元素必须包含签名值、签名算法等信息。

元素	说明
Subject	Subject 必须包含以下元素： ○ 有且仅有一个 NameID 元素，是阿里云账号下的某个RAM用户的身份标识。详情请参见本文下面所述的NameID元素和NameID示例。 ○ 有且仅有一个 SubjectConfirmation 元素，其中包含一个 SubjectConfirmationData 元素。 SubjectConfirmationData 必须有以下两个属性： ■ NotOnOrAfter ：规定SAML断言的有效期。 ■ Recipient ：阿里云通过检查该元素的值来确保阿里云是该断言的目标接收方，其取值必须为 https://signin-intl.aliyun.com/saml/SSO 。 以下是一个 Subject 元素的示例： <Subject> <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">Alice@example.onaliyun.com</NameID> <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <SubjectConfirmationData NotOnOrAfter="2019-01-01T00:01:00.000Z" Recipient="https://signin-intl.aliyun.com/saml/SSO"/> </SubjectConfirmation> </Subject>
Conditions	在 Conditions 元素中，必须包含一个 AudienceRestriction 元素，其中可包含一至多个 Audience 元素，但必须有一个 Audience 元素的取值为 https://signin-intl.aliyun.com/${accountId}/saml/SSO ， ${accountId} 为阿里云账号ID。 以下是一个 Conditions 元素的示例： <Conditions> <AudienceRestriction> <Audience>https://signin-intl.aliyun.com/${accountId}/saml/SSO</Audience> </AudienceRestriction> </Conditions>

- **NameID元素**

阿里云需要通过UPN（User Principal Name）来定位一个RAM用户，所以要求企业IdP生成的SAML断言包含用户的UPN。阿里云通过解析SAML断言中的 `NameID` 元素，来匹配RAM用户的UPN从而实现用户SSO。

因此，在配置IdP颁发的SAML断言时，需要将对应于RAM用户UPN的字段映射为SAML断言中的 `NameID` 元素。

`NameID` 元素必须是以下几种：

- 使用**域别名**作为 `NameID` 元素的后缀，即 `<username>@<domain_alias>` 。其中 `<username>` 为RAM用户的用户名， `<domain_alias>` 为域别名。关于如何设置域别名，请参见创建并验证域别名。
- 使用**辅助域名**作为 `NameID` 元素的后缀，即 `<username>@<auxiliary_domain>` 。其中 `<username>` 为RAM用户的用户名， `<auxiliary_domain>` 为辅助域名。关于如何设置辅助域名，请参见进行用户SSO时阿里云SP的SAML配置。

  > **说明** 如果您同时设置了域别名和辅助域名，辅助域名将不会生效。此时， `NameID` 元素只能使用域别名作为后缀。

- 使用**默认域名**作为 `NameID` 元素的后缀，即 `<username>@<default_domain>` 。其中 `<username>` 为RAM用户的用户名， `<default_domain>` 为默认域名。关于如何设置默认域名，请参见查看和修改默认域名。

  > **说明** 即使设置了域别名或辅助域名，仍可以使用默认域名作为 `NameID` 的后缀。

- **NameID示例**

  RAM用户名为 `Alice` ，默认域名为 `example.onaliyun.com` 。

  - 如果设置了域别名为 `example.com` ，SAML断言中的 `NameID` 取值为 `Alice@example.onaliyun.com` 或 `Alice@example.com` 。
  - 如果没有设置域别名，设置了辅助域名为 `example.net` ，SAML断言中的 `NameID` 取值为 `Alice@example.onaliyun.com` 或 `Alice@example.net` 。
  - 如果设置了域别名为 `example.com` 后，又设置了辅助域名为 `example.net` ，SAML断言中的 `NameID` 取值为 `Alice@example.onaliyun.com` 或 `Alice@example.com` 。注意此时辅助域名不生效。

3.5. 使用AD FS进行用户SSO的示例

本文提供一个以AD FS与阿里云进行用户SSO的示例，帮助您理解企业IdP与阿里云进行SSO的端到端配置流程。本文以在Windows Server 2012 R2 ECS实例上搭建的AD FS为例进行介绍。

准备工作

配置SSO登录前，您需要完成以下工作：

1. 在Windows Server 2012 R2 ECS实例上搭建以下服务器。
   - DNS服务器：将身份认证请求解析到正确的Federation Service上。
   - Active Directory域服务（AD DS）：提供对域用户和域设备等对象的创建、查询和修改等功能。
   - Active Directory Federation Service（AD FS）：提供配置SSO信赖方的功能，并对配置好的信赖方提供SSO认证。

> **注意** 本文中涉及到Microsoft Active Directory配置的部分属于建议，仅用于帮助理解阿里云SSO登录的端到端配置流程，阿里云不提供Microsoft Active Directory配置的咨询服务。

2. 规划配置数据。
   - 云账号的默认域名：`secloud.onaliyun.com`。
   - 云账号下包含RAM用户：`alice`，其完整的 UPN（User Principal Name）为`alice@secloud.onaliyun.com`。
   - 创建的Microsoft AD中的AD FS服务名称：`adfs.secloud.club`。
   - 创建的Microsoft AD的域名：`secloud.club`，NETBIOS名为`secloud`。
   - RAM用户`alice`在AD中的UPN：`alice@secloud.club`，域内登录也可以使用`secloud\alice`。

步骤一：在RAM中将AD FS配置为可信SAML IdP

1. 在浏览器中输入如下地址：`https://adfs.secloud.club/FederationMetadata/2007-06/FederationMetadata.xml`。
2. 将元数据XML文件下载到本地。
3. 在RAM控制台的SSO配置时使用下载好的元数据文件。

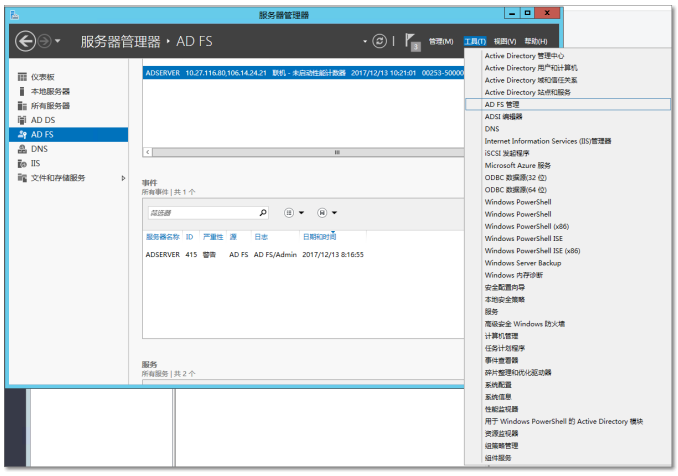
   具体操作，请参见进行用户SSO时阿里云SP的SAML配置。

> **说明** 如果元数据文件超过大小限制，您可以尝试删除`<fed:ClaimTypesRequested>`和`<fed:ClaimTypesOffered>`中的所有内容。

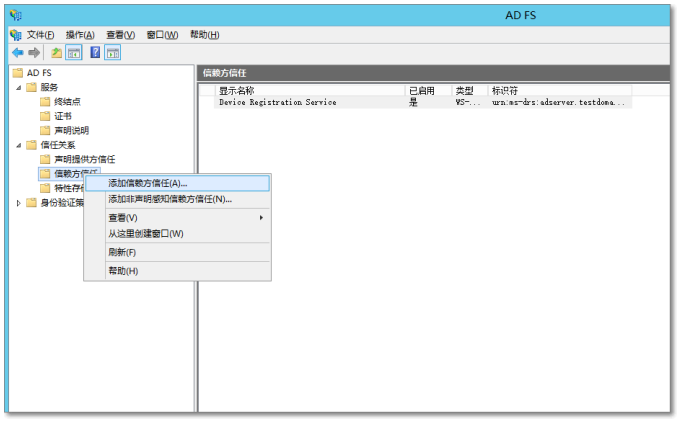
步骤二：在AD FS中将阿里云配置为可信SAML SP

在AD FS中，SAML SP被称作**信赖方**。

1. 在**服务器管理器**的**工具**菜单中选择**AD FS管理**。

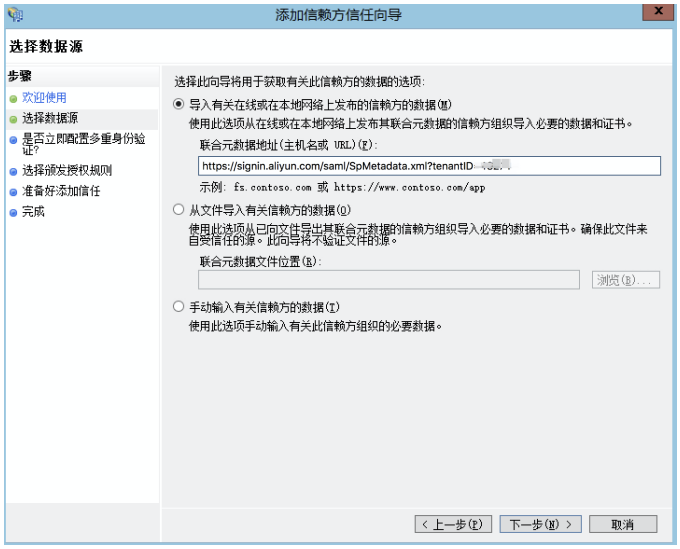


2. 在**AD FS管理**工具中**添加信赖方信任**。



3. 为新创建的信赖方设置阿里云的SAML元数据。

   阿里云账号的SAML服务提供商元数据URL可以登录RAM控制台，在左侧菜单栏，单击**SSO管理**，在**用户SSO**页签下的**SSO登录设置**区域下查看。AD FS信赖方可以直接配置元数据的URL。



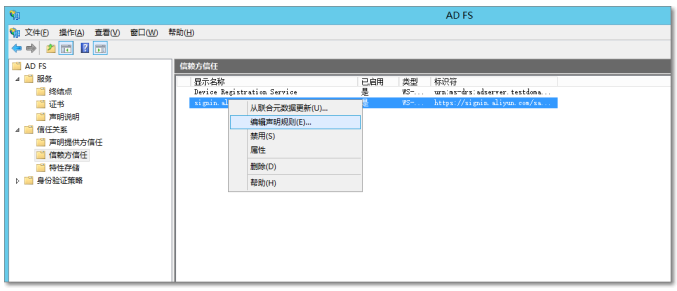
完成配置信赖方之后，阿里云和AD FS就产生了互信，阿里云会将默认域名为 `secloud.onaliyun.com` 的云账号下所有RAM用户的认证请求转发到AD FS： `adfs.secloud.club` ，AD FS也会接受来自于阿里云的认证请求并向阿里云转发认证响应。

步骤三：为阿里云SP配置SAML断言属性

为了让阿里云能使用SAML响应定位到正确的RAM用户，SAML断言中的 `NameID` 字段取值应为RAM用户的UPN。

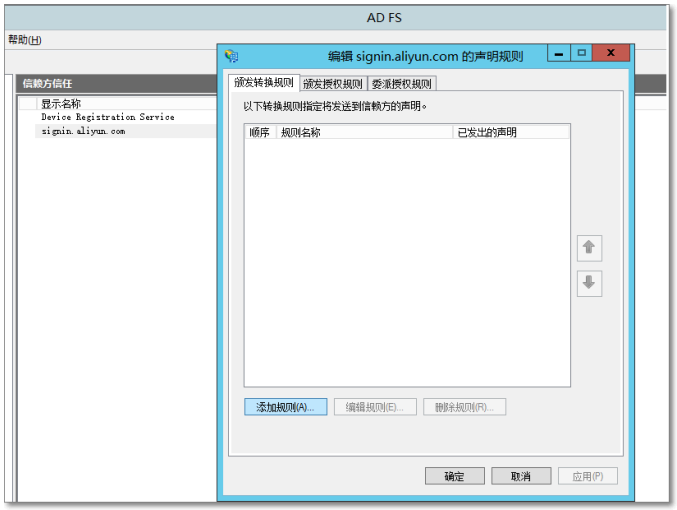
我们需要配置AD中的UPN为SAML断言中的 `NameID` 。

1. 为信赖方**编辑声明规则**。



2. 添加**颁发转换规则**。

> **说明** 颁发转换规则（Issuance Transform Rules）：指如何将一个已知的用户属性，经过转换后颁发为SAML断言中的属性。由于我们要将用户在AD中的UPN颁发为 `NameID` ，因此需要添加一个新的规则。



3. **声明规则模版**选择**转换传入声明**。

4. **编辑规则**。

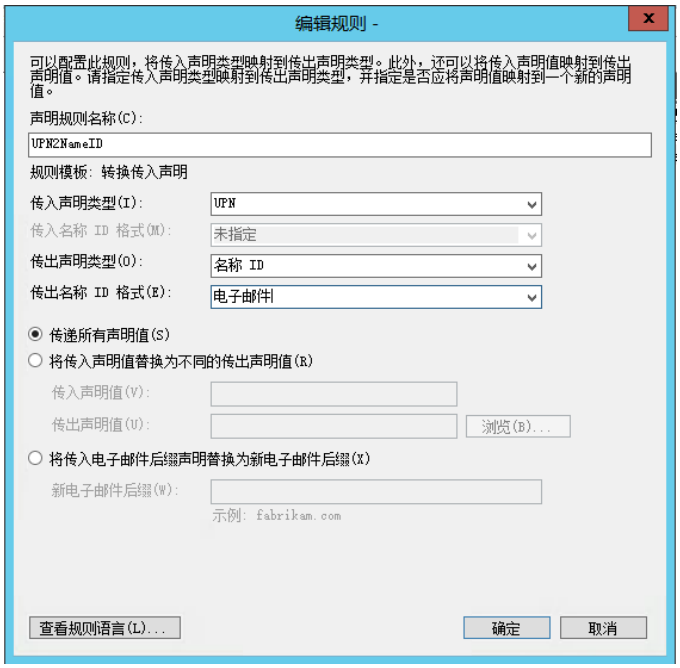
> **说明** 由于示例中的云账号里的UPN域名为 `secloud.onaliyun.com` ，而AD中的UPN域名为 `secloud.club` ，如果直接将AD中的UPN映射为 `NameID` ，阿里云将无法匹配到正确的RAM用户。

下面提供几种设置RAM用户的UPN与AD用户的UPN保持一致的方法：

i. 方法一：将AD域名设置为RAM的**域别名**。

如果AD域名 `secloud.club` 是一个在公网DNS中注册的域名。用户可以将 `secloud.club` 设置为RAM的**域别名**。关于如何设置域别名，请参见创建并验证域别名。

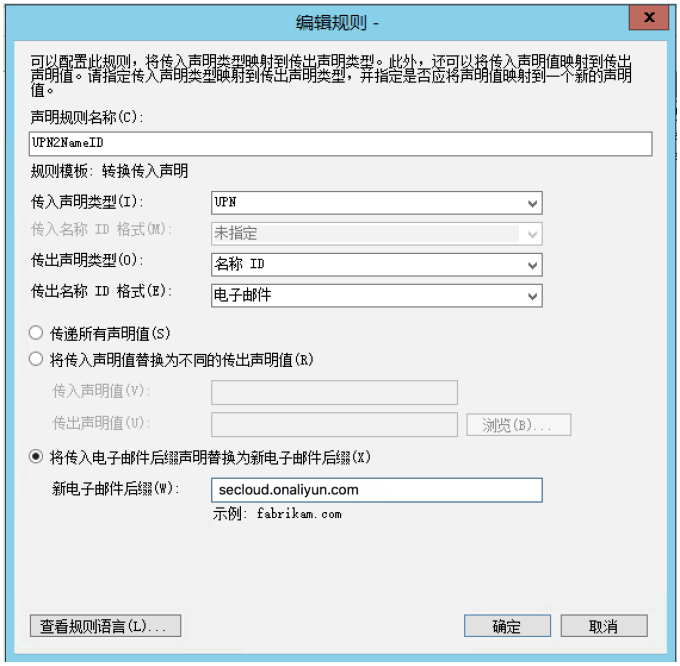
完成设置后，在**编辑规则**对话框，将UPN映射为名称ID（ `NameID` ）。



ii. 方法二：在AD FS中设置域名转换。

如果域名 `secloud.club` 是企业的内网域名，那么阿里云将无法验证企业对域名的所有权。RAM就只能使用默认域名 `secloud.onaliyun.com` 。

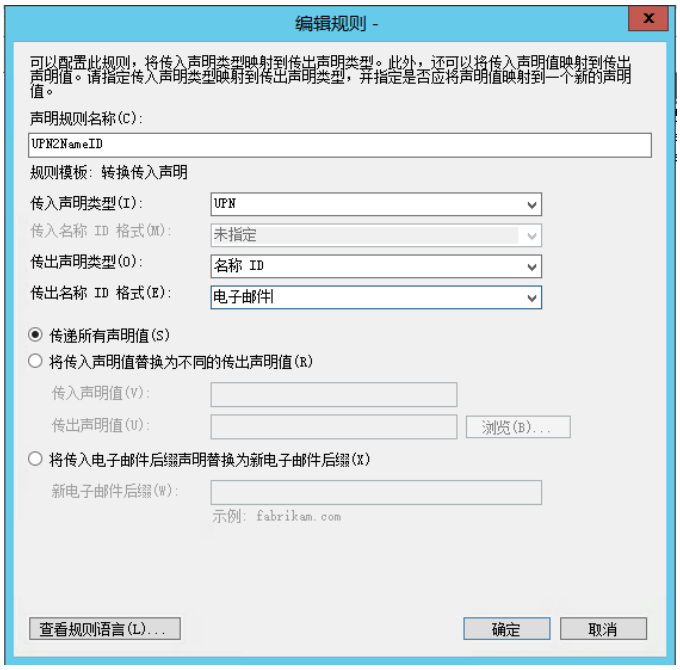
在AD FS给阿里云颁发的SAML断言中必须将UPN的域名后缀从 `secloud.club` 替换为： `secloud.onaliyun.com` 。



iii. 方法三：将AD域名设置为用户SSO的辅助域名。

如果域名 `secloud.club` 是企业的内网域名，那么阿里云将无法验证企业对域名的所有权。您可以将 `secloud.club` 设置为用户SSO的辅助域名，无需进行域名转换。关于如何设置辅助域名，请参见进行用户SSO时阿里云SP的SAML配置。

完成设置后，在**编辑规则**对话框，将UPN映射为名称ID（ `NameID` ）。



3.6. 使用Okta进行用户SSO的示例

本文提供一个以Okta与阿里云进行用户SSO的示例，帮助您理解企业IdP与阿里云进行SSO的端到端配置流程。

步骤一：在阿里云获取SAML服务提供商元数据

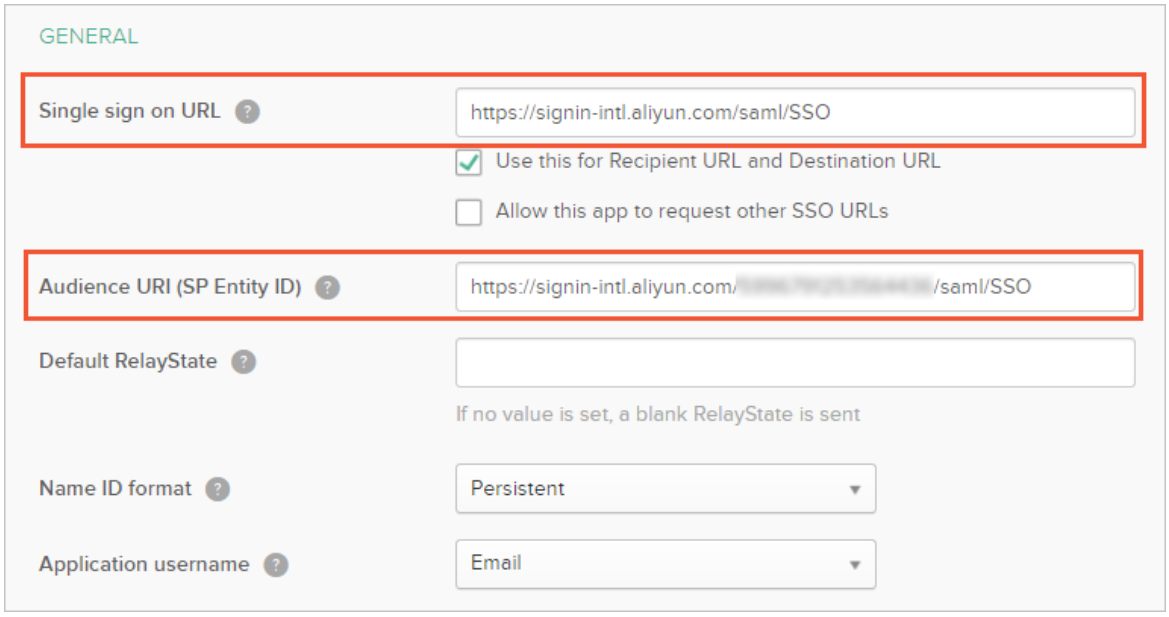
1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**SSO管理**页面，单击**用户SSO**页签。
4. 在**SSO登录设置**区域，复制**SAML服务提供商元数据URL**。
5. 在新的浏览器窗口中打开复制的链接，将元数据XML文件另存到本地。

> **说明** 元数据XML文件保存了阿里云作为一个SAML服务提供商的访问信息。您需要记录XML文件中 `EntityDescriptor` 元素的 `entityID` 属性值和 `AssertionConsumerService` 元素的 `Location` 属性值，以便后续在Okta的配置中使用。

步骤二：在Okta创建支持SAML SSO的应用

1. 登录Okta门户。
2. 单击页面右上方的账号图标，然后单击Your Org。
3. 在左侧导航栏，选择Applications > Applications。

4. 在Applications页面，单击Create App Integration。
5. 在Create a new app integration对话框，单击SAML 2.0，然后单击Next。
6. 配置应用名称为AliyunSSODemo，单击Next。
7. 配置SAML，然后单击Next。



   - Single sign on URL为步骤一：在阿里云获取SAML服务提供商元数据中记录的 `Location` 。
   - Audience URI为步骤一：在阿里云获取SAML服务提供商元数据中记录的 `entityID` 。
   - Default RelayState用来配置用户SSO登录成功后跳转到的阿里云页面。

     > **说明** 出于安全原因，您只能填写阿里巴巴旗下的域名URL作为Default RelayState的值，例如：*.aliyun.com、*.hichina.com、*.yunos.com、*.taobao.com、*.tmall.com、*.alibabacloud.com、*.alipay.com，否则配置无效。若不配置，默认跳转到阿里云控制台首页。

   - Name ID format选择Persistent。
   - Application username选择Email。
8. 在Feedback页面，根据需要选择合适的应用类型，然后单击Finish。

步骤三：在Okta获取SAML IdP元数据

1. 在应用程序AliyunSSODemo详情页，单击Sign On。
2. 在Settings区域，单击Identity Provider metadata，将IdP元数据另存到本地。

步骤四：在阿里云开启用户SSO

1. 在RAM控制台的左侧导航栏，单击SSO管理。
2. 在SSO管理页面，单击用户SSO页签。
3. 在SSO登录设置区域，单击编辑。
4. 在编辑SSO登录设置面板的SSO功能状态区域，单击开启。

> **说明** 用户SSO是一个全局功能，开启后，所有RAM用户都需要使用SSO登录。如果您是通过RAM用户配置的，请先保留为关闭状态，您需要先完成RAM用户的创建，以免配置错误导致自己无法登录。您也可以通过阿里云账号（主账号）进行配置来规避此问题。

5. 在**元数据文档**区域，单击**上传文件**，上传从步骤三：在Okta获取SAML IdP元数据中获取的IdP元数据。
6. 在**辅助域名**区域，单击**开启**，并配置辅助域名为Okta中的用户名Email后缀。

> **说明** 如果您的Okta中存在多种Email后缀的用户，则只有以此处配置的后缀结尾的Email地址可以登录到阿里云。

7. 单击**确定**。

步骤五：在Okta创建用户并分配应用

1. 在Okta左侧导航栏，选择**Directory > People**。
2. 单击**Add Person**。
3. 在**Add Person**页面，填写基本信息并将**Primary email**配置为u2@example.com，然后单击**Save**。
4. 在用户列表中，单击用户u2@example.com**Status**列的**Activate**，然后根据页面提示激活u2@example.com。
5. 在左侧导航栏，选择**Applications > Applications**。
6. 单击目标应用名称（AliyunSSODemo）后，在**Assignments**页签，选择**Assign > Assign to People**。
7. 单击目标用户（u2@example.com）后的**Assign**。
8. 单击**Save and Go Back**。
9. 单击**Done**。

步骤六：在阿里云创建RAM用户

1. 在RAM控制台的左侧导航栏，选择**身份管理 > 用户**。
2. 在**用户**页面，单击**创建用户**。
3. 在**创建用户**页面，输入**登录名称**和**显示名称**。

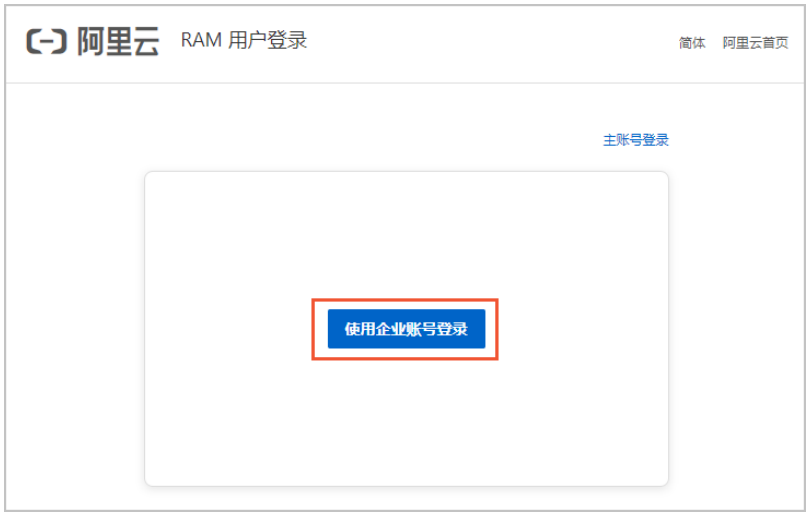
> **说明** 请确保RAM用户的登录名称前缀与Okta中的用户名前缀保持一致，本示例中为u2。

4. 在**访问方式**区域，选择**控制台访问**，并设置登录密码等参数。
5. 单击**确定**。

验证结果

完成上述配置后，您可以从阿里云或Okta发起SSO登录。

- 从阿里云侧发起登录
  i. 在RAM控制台的**概览**页，复制RAM用户的登录地址。
  ii. 将鼠标悬停在右上角头像的位置，单击**退出登录**或使用新的浏览器打开复制的RAM用户登录地址。
  iii. 单击**使用企业账号登录**，系统会自动跳转到Okta的登录页面。



iv. 在Okta的登录界面，输入用户名（u2@example.com）和密码，单击**登录**。

系统将自动SSO登录并重定向到您指定的DefaultRelayState页面。如果未指定DefaultRelayState或超出允许范围，则系统会访问如下阿里云控制台首页。如果出现以下页面，表示配置成功。

- 从Okta侧发起登录

使用Okta用户登录Okta门户，在Okta的主页，找到并单击AliyunSSODemo应用。

系统将自动SSO登录并重定向到您指定的DefaultRelayState页面。如果未指定DefaultRelayState或超出允许范围，则系统会访问以下阿里云控制台首页。如果出现以下页面，表示配置成功。

3.7. 使用Azure AD进行用户SSO的示例

本文提供一个以Azure AD（Azure Active Directory，以下简称 AAD）与阿里云进行用户SSO的示例，帮助您理解企业IdP与阿里云进行SSO的端到端配置流程。

背景信息

在本示例中，企业拥有一个阿里云账号和一个Azure AD租户。在Azure AD租户中，您有一个管理员用户（已授予全局管理员权限）和一个企业员工用户（u2）。您希望经过配置，使企业员工用户（u2）在登录Azure AD后，通过用户SSO访问阿里云。

您需要通过管理员用户（已授予全局管理员权限）执行本示例AAD中的操作。关于如何在AAD中创建用户和为用户授权，请参见AAD文档。

步骤一：在阿里云获取SAML服务提供商元数据

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**SSO管理**页面，单击**用户SSO**页签。
4. 在**SSO登录设置**区域，复制**SAML服务提供商元数据URL**。
5. 在新的浏览器窗口中打开复制的链接，将元数据XML文件另存到本地。

> **说明** 元数据XML文件保存了阿里云作为一个SAML服务提供商的访问信息。您需要记录该文件中的 `entityID` 和 `Location` 的值，以便后续在AAD的配置中使用。

步骤二：在AAD中创建应用

1. 管理员用户登录Azure门户。
2. 单击主页的图标。
3. 在左侧导航栏，选择**Azure Active Directory > 企业应用程序 > 所有应用程序**。
4. 单击**新建应用程序**。
5. 在**浏览Azure AD库**页面，单击**创建你自己的应用程序**。
6. 在**创建你自己的应用程序**页面，输入应用名称（例如：AliyunSSODemo），并选择**集成库中未发现的任何其他应用程序（非库）**，然后单击**创建**。

步骤三：在AAD中配置SAML

1. 在**AliyunSSODemo**页面，单击左侧导航栏的**单一登录**。
2. 在**选择单一登录方法**页面，单击**SAML**。
3. 在**设置SAML单一登录**页面进行以下配置。
   i. 在页面左上角，单击**上载元数据文件**，选择文件后，单击**添加**。

> **说明** 此处上传步骤一：在阿里云获取SAML服务提供商元数据中获取的XML文件。

ii. 在**基本SAML配置**页面，配置以下信息，然后单击**保存**。

- **标识符（实体 ID）**：从上一步的元数据文件中自动读取 `entityID` 的值。
- **回复 URL（断言使用者服务 URL）**：从上一步的元数据文件中自动读取 `Location` 的值。
- **中继状态**：用来配置用户SSO登录成功后跳转到的阿里云页面。

> **说明** 出于安全原因，您只能填写阿里巴巴旗下的域名URL作为**中继状态**的值，例如：*.aliyun.com、*.hichina.com、*.yunos.com、*.taobao.com、*.tmall.com、*.alibabacloud.com、*.alipay.com，否则配置无效。若不配置，默认跳转到阿里云控制台首页。

iii. 在**SAML签名证书**区域，单击**下载**，获取**联合元数据XML**。

步骤四：在AAD分配用户

1. 单击AAD主页的☰图标。
2. 在左侧导航栏，选择**Azure Active Directory > 企业应用程序 > 所有应用程序**。
3. 在**名称**列，单击**AliyunSSODemo**。
4. 在左侧导航栏，单击**用户和组**。
5. 单击左上角的**添加用户/组**。
6. 单击**用户**，从用户列表中选择用户（u2），然后单击**选择**。
7. 单击**分配**。

步骤五：在阿里云创建RAM用户

1. 在RAM控制台的左侧导航栏，选择**身份管理 > 用户**。
2. 在**用户**页面，单击**创建用户**。
3. 在**创建用户**页面的**用户账号信息**区域，输入**登录名称**和**显示名称**。

   请确保RAM用户登录名称前缀与AAD中的用户名前缀保持一致。本示例中为u2。
4. 在**访问方式**区域，选择访问方式。
5. 单击**确定**。

步骤六：在阿里云开启用户SSO

1. 在RAM控制台的左侧导航栏，单击**SSO管理**。
2. 在**SSO管理**页面，单击**用户SSO**页签。
3. 在**SSO登录设置**区域，单击**编辑**。
4. 在**编辑SSO登录设置**面板的**SSO功能状态**区域，单击**开启**。

> **说明** 用户SSO是一个全局功能，开启后，所有RAM用户都需要使用SSO登录。如果您是通过RAM用户配置的，请先保留为关闭状态，您需要先完成RAM用户的创建，以免配置错误导致自己无法登录。您也可以通过阿里云账号进行配置来规避此问题。

5. 在**元数据文档**区域，单击**上传文件**，上传从步骤三：在AAD中配置SAML中获取的XML文件。
6. 在**辅助域名**区域，单击**开启**，并配置辅助域名为AAD中的用户名Email后缀。

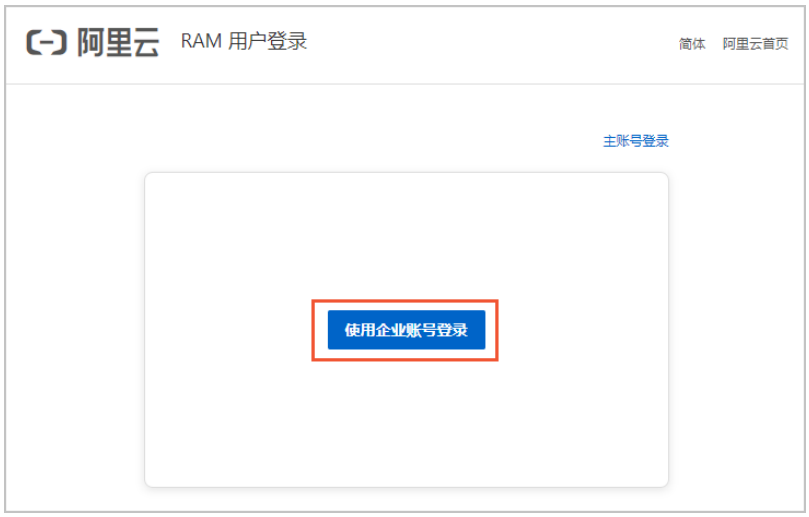
例如：本示例中AAD用户（u2）的完整用户名为u2@test.onmicrosoft.com，则此处填写test.onmicrosoft.com。

7. 单击**确定**。

验证结果

完成SSO登录配置后，您可以从阿里云或AAD发起SSO登录。

- 从阿里云侧发起登录
  i. 在RAM控制台的**概览**页，复制RAM用户的登录地址。
  ii. 将鼠标悬停在右上角头像的位置，单击**退出登录**或使用新的浏览器打开复制的RAM用户登录地址。
  iii. 单击**使用企业账号登录**，系统会自动跳转到AAD的登录页面。



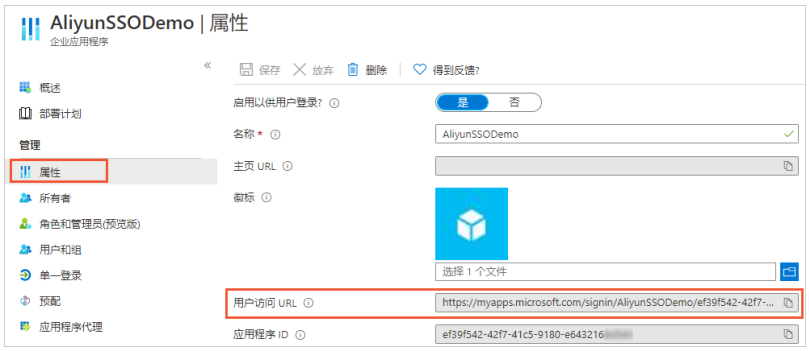
  iv. 使用用户（u2）的用户名和密码登录。

  系统将自动SSO登录并重定向到您指定的**中继状态**页面。如果未指定**中继状态**或超出允许范围，则系统会访问以下阿里云控制台首页。

- 从AAD侧发起登录
  i. 获取用户访问URL
    a. 管理员用户登录Azure门户。
    b. 单击主页的☰图标。
    c. 在左侧导航栏，选择**Azure Active Directory > 企业应用程序 > 所有应用程序**。
    d. 单击应用程序**AliyunSSODemo**。

e. 在左侧导航栏，单击**属性**，获取**用户访问URL**。

用户访问URL是用户直接从其浏览器访问此应用程序的链接。



ii. 用户（u2）从管理员用户处获取上述**用户访问URL**在浏览器中输入该URL，使用自己的账号登录。

系统将自动SSO登录并重定向到您指定的**中继状态**页面。如果未指定**中继状态**或超出允许范围，则系统会访问以下阿里云控制台首页。

4.角色SSO

4.1. 基于SAML的角色SSO

4.1.1. SAML角色SSO概览

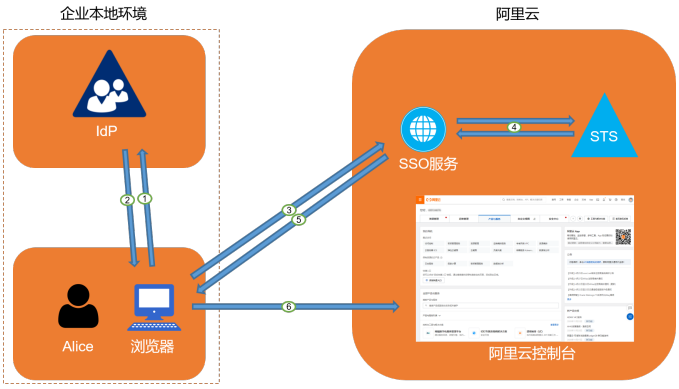
阿里云与企业进行角色SSO时，阿里云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过角色SSO，企业可以在本地IdP中管理员工信息，无需进行阿里云和企业IdP间的用户同步，企业员工将使用指定的RAM角色登录阿里云。

基本流程

企业员工可以通过控制台或程序访问阿里云。

- **通过控制台访问阿里云**

  当管理员在完成角色SSO的相关配置后，企业员工Alice可以通过如下图所示的方法登录到阿里云。



  操作步骤：

  i. Alice使用浏览器在IdP的登录页面中选择阿里云作为目标服务。

     例如：如果企业IdP使用AD FS（Microsoft Active Directory Federation Service），则登录URL为：`https://ADFSServiceName/adfs/ls/IdpInitiatedSignOn.aspx`。

     > **说明** 有些IdP会要求用户先登录，再选择代表阿里云的SSO应用。

  ii. IdP生成一个SAML响应并返回给浏览器。

  iii. 浏览器重定向到SSO服务页面，并转发SAML响应给SSO服务。

  iv. SSO服务使用SAML响应向阿里云STS服务请求临时安全凭证，并生成一个可以使用临时安全凭证登录阿里云控制台的URL。

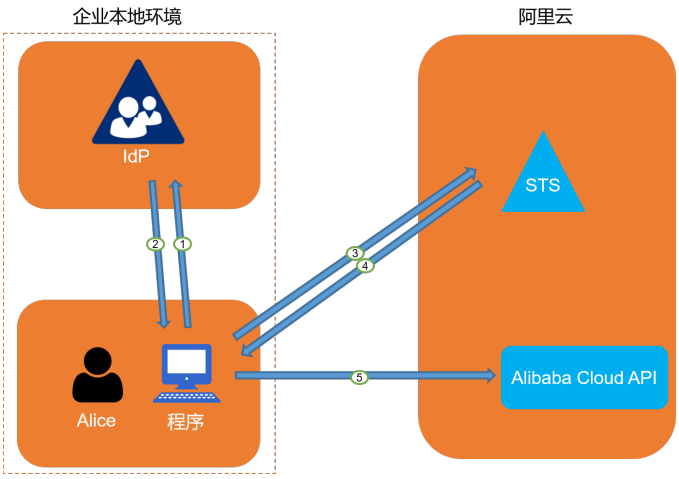
     > **说明** 如果SAML响应中包含映射到多个RAM角色的属性，系统将会首先提示用户选择一个用于访问阿里云的角色。

  v. SSO服务将URL返回给浏览器。

  vi. 浏览器重定向到该URL，以指定RAM角色登录到阿里云控制台。

- **通过程序访问阿里云**

  企业员工Alice可以通过编写程序来访问阿里云，基本流程如下图所示。



操作步骤：

i. Alice使用程序向企业IdP发起登录请求。

ii. IdP生成一个SAML响应，其中包含关于登录用户的SAML断言，并将此响应返回给程序。

iii. 程序调用阿里云STS服务提供的API AssumeRoleWithSAML，并传递以下信息：

阿里云中身份提供商的ARN、要扮演的角色的ARN以及来自企业IdP的SAML断言。

iv. STS服务将校验SAML断言并返回临时安全凭证给程序。

v. 程序使用临时安全凭证调用阿里云API。

配置步骤

为了建立阿里云与企业IdP之间的互信关系，需要进行阿里云作为SP的SAML配置和企业IdP的SAML配置，配置完成后才能进行角色SSO。

1. 为了建立阿里云对企业IdP的信任，需要将企业IdP配置到阿里云。

   更多信息，请参见进行角色SSO时阿里云SP的SAML配置。

2. 企业需要RAM控制台或程序创建用于SSO的RAM角色，并授予相关权限。

   更多信息，请参见创建可信实体为身份提供商的RAM角色。

3. 为了建立企业IdP对阿里云的信任，需要在企业IdP中配置阿里云为可信SAML SP并进行SAML断言属性的配置。

   更多信息，请参见进行角色SSO时企业IdP的SAML配置。

配置示例

以下为您提供了常见的企业IdP（例如：AD FS、Okta、Azure AD和OneLogin）与阿里云进行角色SSO的配置示例：

- 使用AD FS进行角色SSO的示例
- 使用Okta进行角色SSO的示例
- 使用Azure AD进行角色SSO的示例
- 使用OneLogin进行角色SSO的示例

4.1.2. SAML身份提供商

4.1.2.1. 创建SAML身份提供商

在使用SAML角色SSO时，需要创建身份提供商。

前提条件

请确保已获取到企业IdP的元数据文档。元数据文档为XML格式，包含IdP的登录服务地址、用于验证签名的公钥及断言格式等信息。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**SAML**页签，然后单击**创建身份提供商**。
4. 在**创建身份提供商**页面，输入**身份提供商名称**和**备注**。
5. 在**元数据文档**区域，单击**上传文件**，上传从企业IdP获取的元数据文档。
6. 单击**确定**。

后续步骤

单击**前往新建RAM角色**可直接跳转到RAM角色管理页面。关于如何创建RAM角色，请参见创建可信实体为身份提供商的RAM角色。

4.1.2.2. 查看SAML身份提供商基本信息

本文为您介绍如何查看SAML身份提供商基本信息，包括身份提供商名称、身份提供商类型、创建时间、更新时间、ARN和备注。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**SAML**页签，然后单击目标身份提供商名称。
4. 在**身份提供商信息**区域，查看**身份提供商名称**、**身份提供商类型**、**创建时间**、**更新时间**、**ARN**和**备注**。

4.1.2.3. 修改SAML身份提供商基本信息

本文为您介绍如何修改SAML身份提供商基本信息，只能修改备注和元数据文档，其他信息都不允许修改。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**SAML**页签，然后单击目标身份提供商名称。
4. 单击**备注**右侧的**编辑**，修改备注。
5. 单击**替换元数据**，重新上传元数据文档。

4.1.2.4. 删除SAML身份提供商

如果不再需要SAML身份提供商，可以将其删除。删除SAML身份提供商后，企业将无法与阿里云RAM进行SAML角色SSO。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**SAML**页签，然后单击目标身份提供商**操作**列的**删除**。
4. 在**删除身份提供商**对话框，单击**确定**。

4.1.3. 进行角色SSO时阿里云SP的SAML配置

进行角色SSO时，为了建立阿里云对企业IdP的信任，需要将企业IdP元数据配置到阿里云。

前提条件

请确保已获取到企业IdP的元数据文档。元数据文档为XML格式，包含IdP的登录服务地址、用于验证签名的公钥及断言格式等信息。

操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**SAML**页签，然后单击**创建身份提供商**。
4. 在**创建身份提供商**页面，输入**身份提供商名称**和**备注**。
5. 在**元数据文档**区域，单击**上传文件**，上传从企业IdP获取的元数据文档。
6. 单击**确定**。

后续步骤

单击**前往新建RAM角色**可直接跳转到RAM角色管理页面。关于如何创建RAM角色，请参见创建可信实体为身份提供商的RAM角色。

4.1.4. 进行角色SSO时企业IdP的SAML配置

进行角色SSO时，为了建立企业IdP对阿里云的信任，需要在企业IdP中配置阿里云为可信SAML服务提供商（SP）。

操作步骤

1. 从阿里云获取SAML服务提供商元数据URL。

   URL为 `https://signin.alibabacloud.com/saml-role/sp-metadata.xml` 。
2. 在企业IdP中创建一个SAML SP，并根据实际情况选择下面任意一种方式配置阿里云为信赖方。
   - 直接使用步骤所述的阿里云元数据URL进行配置。
   - 如果您的IdP不支持URL配置，您可以从步骤所述URL下载元数据文件，并上传至您的IdP。
   - 如果您的IdP不支持元数据文件上传，则需要手动配置以下参数：

- `Entity ID`：`urn:alibaba:cloudcomputing:international`
- `ACS URL`：`https://signin.alibabacloud.com/saml-role/sso`
- `RelayState`（可选）：如果您的IdP支持设置`RelayState`参数，您可以将其配置成SSO登录成功后希望跳转到的页面URL。如果不进行配置，SSO登录成功后，将会跳转到阿里云控制台首页。

  > **说明** 出于安全原因，您只能填写阿里巴巴旗下的域名URL作为`RelayState`的值，例如：*.aliyun.com、*.hichina.com、*.yunos.com、*.taobao.com、*.tmall.com、*.alibabacloud.com、*.alipay.com。

后续步骤

在企业IdP中配置阿里云为可信SAML SP后，需要在企业IdP中配置SAML断言属性。更多信息，请参见角色SSO的SAML响应。

4.1.5. 角色SSO的SAML响应

本文为您介绍进行角色SSO时SAML响应中必须包含的元素，尤其是SAML断言中的元素。

背景信息

在基于SAML 2.0的SSO流程中，当企业用户在IdP登录后，IdP将根据SAML 2.0 HTTP-POST绑定的要求生成包含SAML断言的认证响应，并由浏览器（或程序）自动转发给阿里云。这个SAML断言会被用来确认用户登录状态并从中解析出登录的主体。因此，断言中必须包含阿里云要求的元素，否则登录用户的身份将无法被确认，导致SSO失败。

SAML响应

请确保您的IdP向阿里云发出符合如下要求的SAML响应，每一个元素都必须要有，否则SSO将会失败。

```
<saml2p:Response>
    <saml2:Issuer>...</saml2:Issuer>
    <saml2p:Status>
        ...
    </saml2p:Status>
    <saml2:Assertion>
        <saml2:Issuer>...</saml2:Issuer>
        <ds:Signature>
            ...
        </ds:Signature>
        <saml2:Subject>
            <saml2:NameID>${NameID}</saml2:NameID>
            <saml2:SubjectConfirmation>
                ...
            </saml2:SubjectConfirmation>
        </saml2:Subject>
        <saml2:Conditions>
            <saml2:AudienceRestriction>
                <saml2:Audience>${Audience}</saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement>
            ...
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>
            <saml2:Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/RoleSessionN
ame">
                ...
            </saml2:Attribute>
            <saml2:Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/Role">
                ...
            </saml2:Attribute>
        </saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

SAML断言中的元素说明

- **SAML 2.0协议的通用元素**

元素	说明
`Issuer`	`Issuer` 的值必须与您在阿里云创建的**身份提供商**实体中上传的IdP元数据文件中的 `EntityID` 匹配。
`Signature`	阿里云要求SAML断言必须被签名以确保没有篡改， `Signature` 及其包含的元素必须包含签名值、签名算法等信息。

元素	说明

`Subject`	`Subject` 必须包含以下元素：
	○ 有且仅有一个 `NameID` 元素。您必须按照SAML 2.0协议的要求自定义 `NameID` 的值，通常为SAML断言主体在IdP中的身份标识，阿里云不会依赖该元素的值来确认登录主体。
	○ 有且仅有一个 `SubjectConfirmation` 元素，其中包含一个 `SubjectConfirmationData` 元素。 `SubjectConfirmationData` 必须有以下两个属性：
	■ `NotOnOrAfter` ：规定SAML断言的有效期。
	■ `Recipient` ：阿里云通过检查该元素的值来确保阿里云是该断言的目标接收方，其取值必须为 `https://signin.alibabacloud.com/saml-role/sso` 。
	以下是一个 `Subject` 元素的示例：
	`<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`	在 `Conditions` 元素中，必须包含一个 `AudienceRestriction` 元素，其中可包含一至多个 `Audience` 元素，但必须有一个 `Audience` 元素的取值为 `urn:alibaba:cloudcomputing:international` 。
	以下是一个 `Conditions` 元素的示例：
	`<Conditions>`
	`<AudienceRestriction>`
	`<Audience>urn:alibaba:cloudcomputing:international</Audience>`
	`</AudienceRestriction>`
	`</Conditions>`

- **阿里云要求的自定义元素**

  在SAML断言的 `AttributeStatement` 元素中，必须包含以下阿里云要求的 `Attribute` 元素：

- `Name`属性值为`https://www.aliyun.com/SAML-Role/Attributes/Role`的`Attribute`元素

  该元素为必选，可以有多个。其包含的`AttributeValue`元素取值代表允许当前用户扮演的角色，取值的格式是由角色ARN与身份提供商ARN组合而成的，中间用半角逗号（,）隔开。这两个ARN您可以在控制台获取：

  - 角色ARN：在**角色**页面，单击RAM角色名称，然后在**基本信息**区域查看对应的ARN。
  - 身份提供商ARN：在**SSO管理页面**的**角色SSO**页签下，单击身份提供商名称，然后在**身份提供商信息**区域查看对应的ARN。

  > **说明** 如果是多个，当使用控制台登录时，将会在界面上列出所有角色供用户选择。

  以下是一个Role `Attribute`元素示例：

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

  > **说明** `$account_id`是定义角色和身份提供商的阿里云账号ID。

- `Name`属性值为`https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName`的`Attribute`元素

  该元素为必选且只能有一个。其包含的`AttributeValue`元素取值将被用来作为登录用户信息的一部分显示在控制台上和操作审计日志中。如果您有多个用户使用同一个角色，请确保使用可以唯一标识用户的`RoleSessionName`值，以区分不同的用户，如员工ID、Email地址等。

  其`AttributeValue`元素取值要求：长度不少于2个字符且不超过64个字符，只能是英文字母、数字和特殊字符`-_.@=`。

  以下是一个RoleSessionName `Attribute`元素示例：

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

- `Name`属性值为`https://www.aliyun.com/SAML-Role/Attributes/SessionDuration`的`Attribute`元素

  该元素为可选且最多只能有一个。其包含的`AttributeValue`元素取值为整数，单位为秒，最小值为900，最大值不能超过Role元素所代表的角色的最大会话时间。

  以下是一个SessionDuration `Attribute`元素示例：

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

- **登录会话有效期**

通过控制台登录的情况下，通常SAML断言中设置的 `SessionDuration` 值将会被作为会话的有效期。如果您还定义了 `AuthnStatement` 元素的 `SessionNotOnOrAfter` 属性，那么 `SessionDuration` 与 `SessionNotOnOrAfter` 的较小值将会被作为会话的有效期。如果以上两个值均不存在，则会话有效期取角色**最大会话时间**设置的值。登录会话有效期还会受到**登录会话的过期时间**的限制，即最终的登录会话有效期将不会超过此参数设置的值。详情请参见设置RAM用户安全策略、设置角色最大会话时间。

通过程序登录的情况下，如果您在调用AssumeRoleWithSAML时指定了 `DurationSeconds` 参数，同时您还定义了 `AuthnStatement` 元素的 `SessionNotOnOrAfter` 属性，那么 `SessionDuration` 与 `SessionNotOnOrAfter` 的较小值将会被作为STS Token有效期。如果以上两个值均不存在，则有效期取默认值3600秒。

4.1.6. 使用AD FS进行角色SSO的示例

本文提供一个以AD FS与阿里云进行SSO的示例，帮助用户理解企业IdP与阿里云进行SSO的端到端配置流程。本文以在Windows Server 2012 R2 ECS实例上搭建的AD FS为例进行介绍。

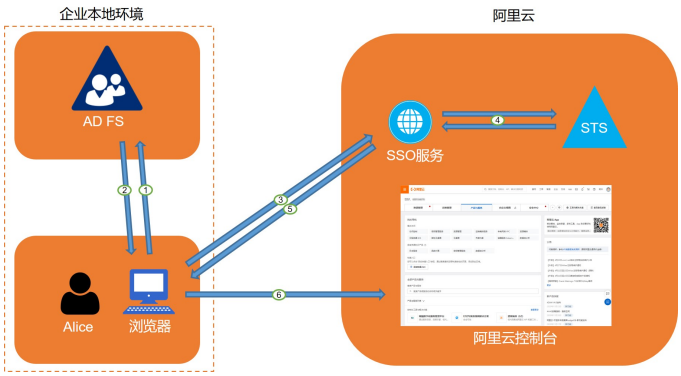
背景信息

企业使用Active Directory（AD）进行员工管理，并通过AD FS配置包括阿里云在内的企业应用。AD管理员通过员工的用户组来管理员工对阿里云账号的访问权限。在本示例中，企业拥有两个阿里云账号（Account1和Account2），要管理的权限为Admin和Reader，企业员工用户名为Alice，该用户所在的AD用户组为Aliyun-<account-id>-ADFS-Admin和Aliyun-<account-id>-ADFS-Reader，企业要实现从AD FS到Account1和Account2的角色SSO。

> **说明**
>
> - <account-id>为云账号Account1或Account2的账号ID，因此用户Alice所在的AD用户组共4个，分别对应两个云账号中的Admin和Reader权限。
> - 本文中涉及到Microsoft Active Directory配置的部分属于建议，仅用于帮助理解阿里云SSO登录的端到端配置流程，阿里云不提供Microsoft Active Directory配置的咨询服务。

基本流程

员工进行控制台登录的基本流程如下图所示。



AD管理员在完成角色联合登录的配置后，企业员工（Alice）可以通过如图所示的方法登录到阿里云控制台。更多信息，请参见SAML角色SSO概览。

上述过程表示，用户登录时，企业会进行统一登录认证，无需用户提供在阿里云上的任何用户名和密码。

步骤一：在阿里云中将AD FS配置为可信SAML IdP

1. 在阿里云RAM控制台，创建身份提供商（ADFS），并配置相应的元数据。AD FS的元数据URL为 `https://<ADFS-server>/federationmetadata/2007-06/federationmetadata.xml` 。

   > **说明** <ADFS-server>是您的AD FS服务器域名或IP地址。

   具体操作，请参见进行角色SSO时阿里云SP的SAML配置。

   > **说明** 如果元数据文件超过大小限制，您可以尝试删除 `<fed:ClaimTypesRequested>` 和 `<fed:ClaimTypesOffered>` 中的所有内容。

2. 在阿里云账号Account1中创建两个可信实体类型为身份提供商的RAM角色（ADFS-Admin和ADFS-Reader），选择刚刚创建的ADFS作为可信身份提供商，并对两个角色分别授予 `AdministratorAccess` 和 `ReadOnlyAccess` 权限。

   具体操作，请参见创建可信实体为身份提供商的RAM角色。

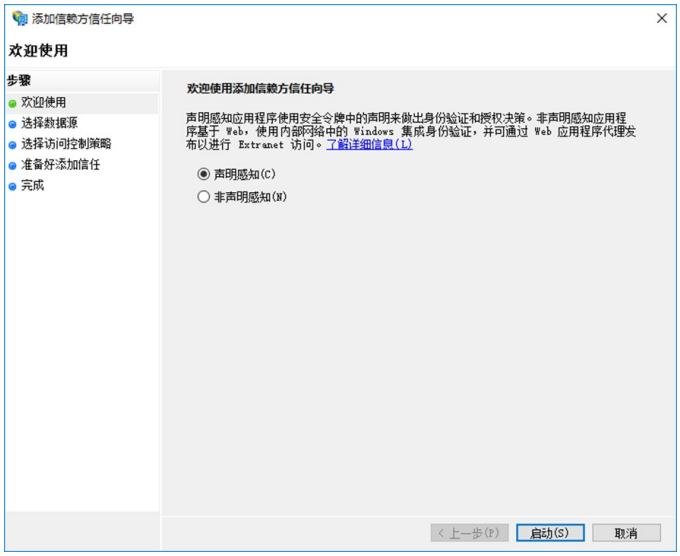
3. 使用同样的方法，在Account2中创建与Account1中同名的身份提供商（ADFS）和角色（ADFS-Admin和ADFS-Reader），并为两个角色分别授予 `AdministratorAccess` 和 `ReadOnlyAccess` 权限。

> **说明** 配置完成后，企业的阿里云账号将信任企业AD FS发来的SAML请求中的用户身份和角色信息。

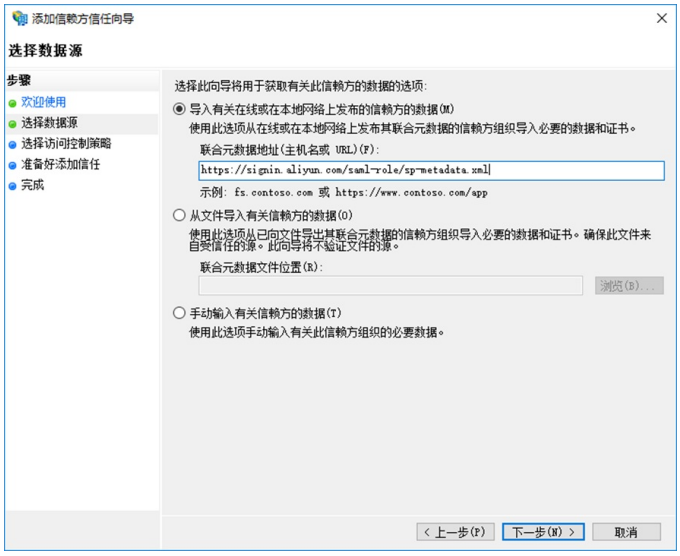
步骤二：在AD FS中将阿里云配置为可信SAML SP

在AD FS中，SAML SP被称作**信赖方（Relying Party）**。设置阿里云作为AD FS的可信SP的操作步骤如下。

1. 在**服务器管理器**的**工具**菜单中选择**AD FS管理**。
2. 在**AD FS**管理工具中**添加信赖方信任**。



3. 为新创建的信赖方设置阿里云的角色SSO的SAML SP元数据，元数据URL为 `https://signin.alibabacloud.com/saml-role/sp-metadata.xml` 。



4. 按照向导完成配置。

步骤三：为阿里云SP配置SAML断言属性

阿里云需要AD FS在SAML断言中提供`NameID`、`Role`和`RoleSessionName`属性。AD FS中通过颁发转换规则来实现这一功能。

- `NameID`

  配置Active Directory中的Windows账户名为SAML断言中的`NameID`，其操作步骤如下。

  i. 为信赖方**编辑声明规则**。

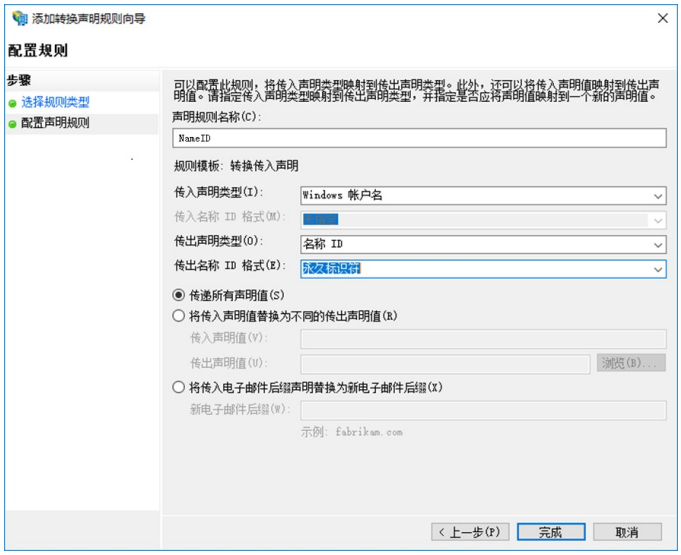
  ii. 添加**颁发转换规则**。

  > **说明** 颁发转换规则（Issuance Transform Rules）：指如何将一个已知的用户属性，经过转换后，颁发为SAML断言中的属性。由于我们要将用户在AD中的Windows账户名颁发为`NameID`，因此需要添加一个新的规则。

  iii. **声明规则模版**选择**转换传入声明**。

  iv. 使用如下配置规则，并单击**完成**。

- **声明规则名称**：NameID
- **传入声明类型**：Windows账户名
- **传出声明类型**：名称ID
- **传出名称ID格式**：永久标识符
- **传递所有声明值**：勾选



配置完成后，AD FS将发送阿里云需要的`NameID`格式。

```
<NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
    YourDomain\rolessouser
</NameID>
```

- `RoleSessionName`

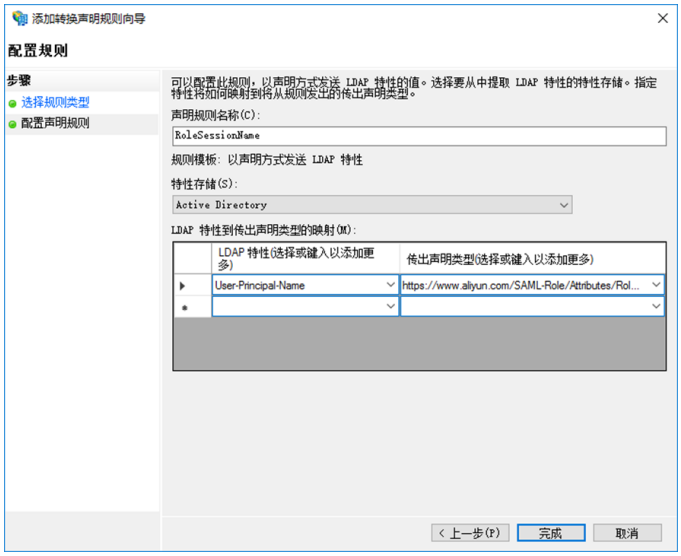
  配置Active Directory中的UPN为SAML断言中的`RoleSessionName`，其操作步骤如下。

  i. 单击**添加转换声明规则**。

  ii. 从**声明规则模板**中选择**以声明方式发送LDAP特性**。

  iii. 使用如下配置规则，并单击**完成**。

- **声明规则名称**：RoleSessionName
- **特性存储**：Active Directory
- **LDAP 特性列**：User-Principal-Name（您也可以根据具体需求选择其他属性，例如email。）
- **传出声明类型**：`https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName`



配置完成后，AD FS将发送阿里云需要的`RoleSessionName`格式。

```
<Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName">
    <AttributeValue>rolessouser@example.com<AttributeValue>
</Attribute>
```

- `Role`

通过自定义规则将特定的用户所属组的信息转化成阿里云上的角色名称，其操作步骤如下。

i. 单击**添加转换声明规则**。

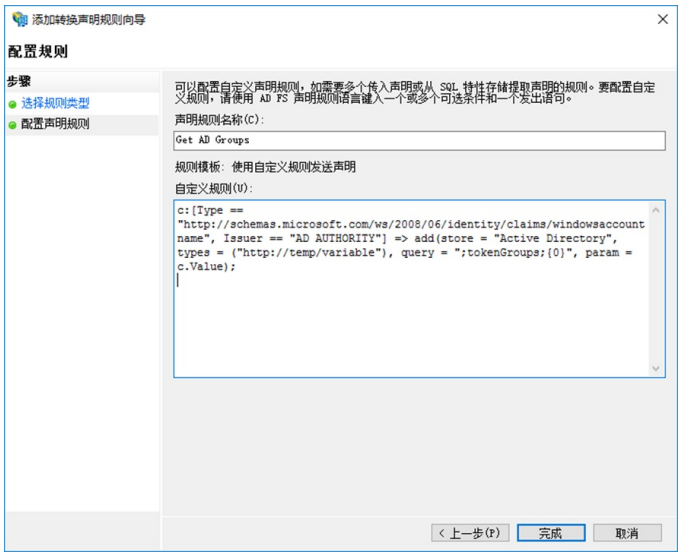
ii. 从**声明规则模板**中选择**使用自定义规则发送声明**，单击**下一步**。

iii. 使用如下配置规则，并单击**完成**。

- **声明规则名称**：Get AD Groups

- **自定义规则**：

```
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);
```



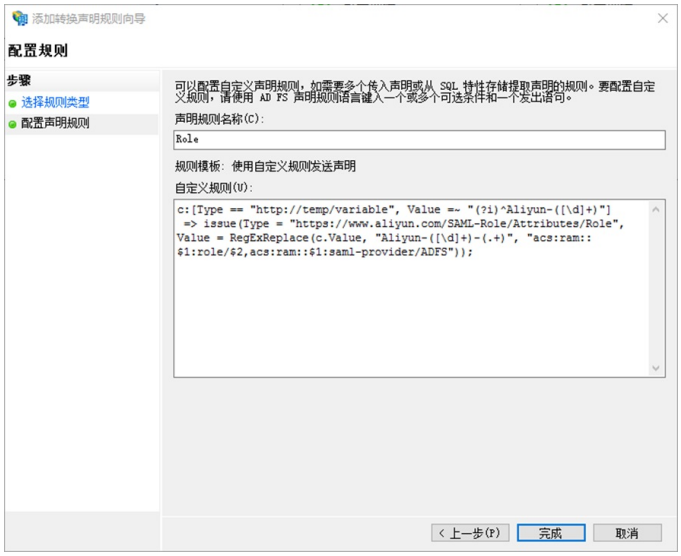
> **说明** 这个规则获取用户在AD中所属组的信息，保存在中间变量*http://temp/variable*中。

iv. 单击**添加转换声明规则**。

v. 重复以上步骤，并单击**完成**。

- **声明规则名称**：Role
- **自定义规则**：

```
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"));
```



> **说明** 根据这个规则，如果用户所属的AD组中包含Aliyun-<account-id>-ADFS-Admin或Aliyun-<account-id>-ADFS-Reader，则将生成一个SAML属性，映射到阿里云上的角色ADFS-Admin或ADFS-Reader。

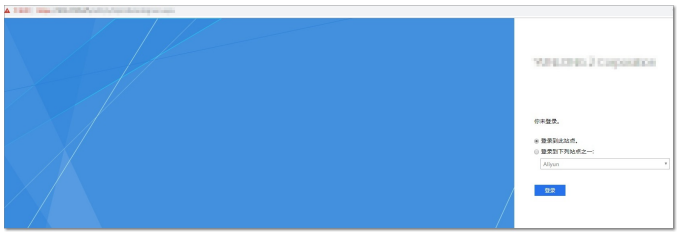
配置完成后，IdP将返回阿里云所需要的SAML断言片段，如下所示。

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

验证结果

1. 登录AD FS SSO门户（URL：`https://<ADFS-server>/adfs/ls/IdpInitiatedSignOn.aspx`），选择阿里云应用，输入用户名密码。

   > **说明** <ADFS-server>是您的AD FS服务器域名或IP地址。如果网页不可用，可以通过PowerShell开启：`Set-AdfsProperties -EnableIdpInitiatedSignonPage $True`。

2. 在阿里云角色SSO页面，选择一个您要登录的角色，单击**登录**。

   > **说明** 如果您的用户在AD中只加入了一个组，则在阿里云上只会对应一个角色，该用户将直接登录，无需选择角色。

4.1.7. 使用Okta进行角色SSO的示例

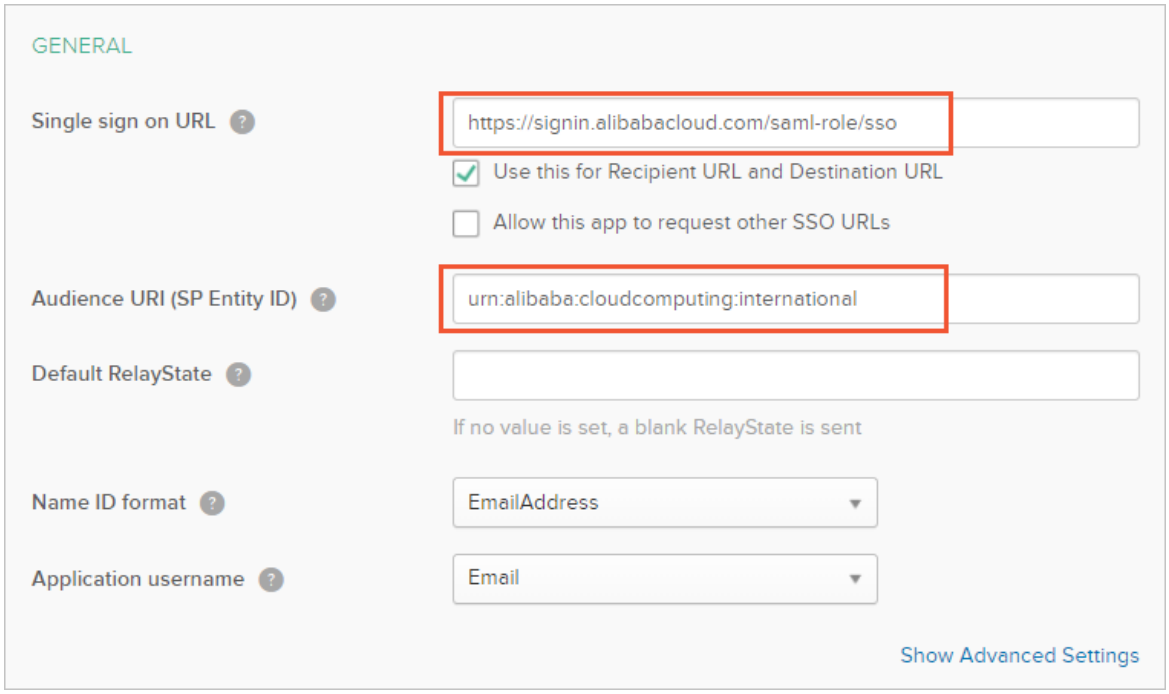
本文提供一个以Okta与阿里云进行角色SSO的示例，帮助您理解企业IdP与阿里云进行SSO的端到端配置流程。

操作流程

本文的配置目标是在Okta应用中创建一个名为approle的属性，并根据这个属性的值来映射访问阿里云的RAM角色。您可以按照下图所示的操作流程完成阿里云、Okta的配置。

步骤一：在Okta创建支持SAML SSO的应用

1. 登录Okta门户。
2. 单击页面右上方的账号图标，然后单击Your Org。
3. 在左侧导航栏，选择Applications > Applications。
4. 在Applications页面，单击Create App Integration。
5. 在Create a new app integration对话框，单击SAML 2.0，然后单击Next。
6. 配置应用名称为role-sso-test，单击Next。
7. 配置SAML，然后单击Next。



- Single sign on URL：`https://signin.alibabacloud.com/saml-role/sso`。
- Audience URI：`urn:alibaba:cloudcomputing:international`。

- Default RelayState：用来配置用户登录成功后跳转到的阿里云页面。

  > **说明** 出于安全原因，您只能填写阿里巴巴旗下的域名URL作为Default RelayState的值，例如：*.aliyun.com、*.hichina.com、*.yunos.com、*.taobao.com、*.tmall.com、*.alibabacloud.com、*.alipay.com，否则配置无效。若不配置，默认跳转到阿里云控制台首页。

- Name ID format：选择EmailAddress。
- Application username：选择Email。

8. 在Feedback页面，根据需要选择合适的应用类型，然后单击Finish。

步骤二：在Okta获取SAML IdP元数据

1. 在应用程序role-sso-test详情页，单击Sign On。
2. 在Settings区域，单击Identity Provider metadata，将IdP元数据另存到本地。

步骤三：在阿里云创建SAML身份提供商

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，单击SAML页签，然后单击**创建身份提供商**。
4. 在**创建身份提供商**页面，输入**身份提供商名称**（okta-provider）和**备注**。
5. 在**元数据文档**区域，单击**上传文件**，上传从步骤二：在Okta获取SAML IdP元数据中获取的IdP元数据。
6. 单击**完成**。
7. 单击**关闭**。

步骤四：在阿里云创建RAM角色

1. 在RAM控制台的左侧导航栏，选择**身份管理 > 角色**。
2. 在**角色**页面，单击**创建角色**。
3. 在**创建角色**面板，选择可信实体类型为**身份提供商**，然后单击**下一步**。
4. 输入**角色名称**（admin）和**备注**。
5. 选择身份提供商类型为**SAML**。
6. 选择从步骤三：在阿里云创建SAML身份提供商中创建的身份提供商并查看限制条件后，然后单击**完成**。
7. 单击**关闭**。

步骤五：在Okta配置Profile

1. 编辑Profile，创建一个新的Attribute。
   i. 在Okta左侧导航栏，选择Directory > Profile Editor。
   ii. 单击对应Profile后面的 Profile 图标。

iii. 单击Add Attribute，填写Attribute信息。

- Data type：选择string。
- Display name：填写将在用户界面中显示的名称，本示例中请填写 `approle` 。
- Variable name：填写将在映射中引用的变量名称，本示例中请填写 `approle` 。您需要记录该参数的值，下一步配置Attribute的时候会用到。
- Description：请根据需要填写属性描述，可以不填写。
- Enum：选中Define enumerated list of values，定义一个枚举值列表。

> **说明** 我们使用Enum来确保用户只能使用预定义的属性值。您也可以不使用Enum，而获得更高的灵活性。

- Attribute members：填写枚举值列表，Value必须要与RAM中创建的角色名称相同，例如：admin、reader。
- Attribute Length：本示例使用枚举值，因此不需要设置。如果您实际中未使用枚举值，请根据需要设置属性长度。
- Attribute required：选中Yes。
- Scope：取消选中User personal。

iv. 单击Save。

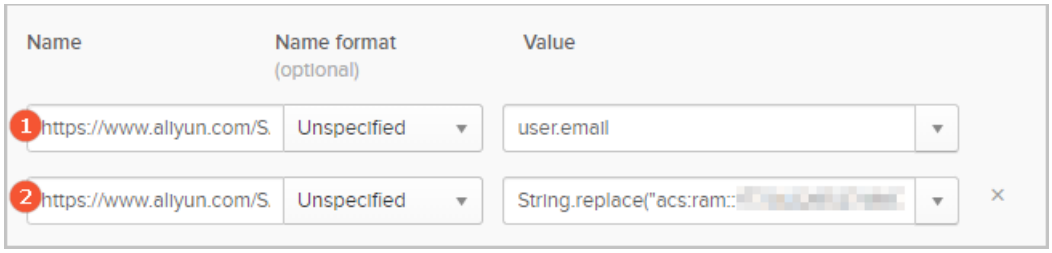
2. 配置Attribute。

i. 在Okta左侧导航栏，选择Applications > Applications。

ii. 单击应用名称role-sso-test。

iii. 在General页签下的SAML Settings区域，单击Edit 。

iv. 在Configure SAML页面的Attribute Statements (optional)区域，配置如下图所示的两条数据。



- 配置第1条数据：
  - Name：填写 `https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName` 。
  - Value：选择user.email。
- 配置第2条数据：
  - Name：填写 `https://www.aliyun.com/SAML-Role/Attributes/Role` 。
  - Value：取值为 `String.replace("acs:ram::<account_id>:role/$approle,acs:ram::<account_id>:saml-provider/okta-provider", "$approle", appuser.approle)` ，是用登录用户在应用Profile中的 `approle` 属性值来替换 `$approle` 占位符，从而获取最终的SAML属性值。其中 `approle` 是之前在Profile Attribute中定义的属性。 `okta-provider` 是步骤三：在阿里云创建SAML身份提供商中创建的身份提供商。 `<account_id>` 需要替换为您的阿里云账号ID。例如： `String.replace("acs:ram::177242285274****:role/$approle,acs:ram::177242285274****:saml-provider/okta-provider", "$approle", appuser.approle)` 。

步骤六：在Okta创建用户并分配应用

1. 创建用户。
   i. 在Okta左侧导航栏，选择Directory > People。
   ii. 单击Add Person。
   iii. 在Add Person页面，填写基本信息并将Primary email配置为被邀请用户的Email，例如：username@example.com，然后单击Save。
   iv. 在用户列表中，单击用户username@example.com Status列的Activate，然后根据页面提示激活username@example.com。
2. 分配应用。

   分配应用有以下两者方式，请任选其一。

   - 为单个用户分配应用。
     a. 在Okta左侧导航栏，选择Applications > Applications。
     b. 单击目标应用名称role-sso-test后，在Assignments页签下，选择Assign > Assign to People。
     c. 单击目标用户username@example.com后的Assign。
     d. 选择approle为admin。
     e. 单击Save and Go Back。
     f. 单击Done。
   - 将用户加入组，为组分配应用。
     a. 在Okta左侧导航栏，先选择Directory > Groups，然后单击Add Group，创建一个组。

b. 单击组名称，然后单击**Manage People**，添加用户到组中。

c. 在Okta左侧导航栏，选择**Applications > Applications**。

d. 单击目标应用名称role-sso-test后，在**Assignments**页签下，单击**Assign > Assign to Groups**。

e. 单击目标组后的**Assign**。

f. 选择**approle**为admin。

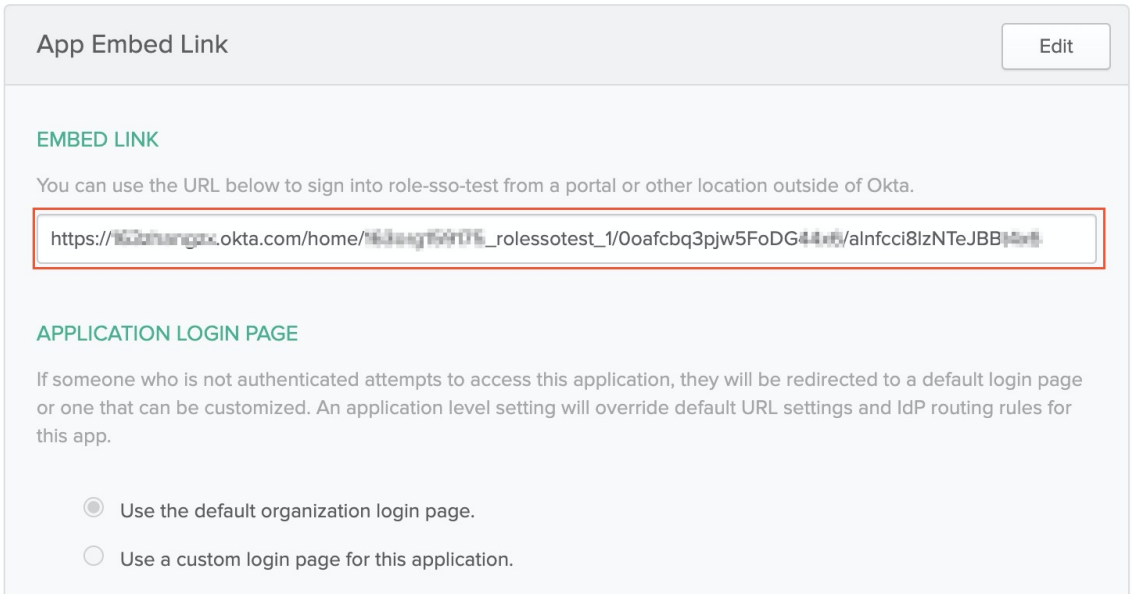
g. 单击**Save and Go Back**。

h. 单击**Done**。

> **说明** 如果一个用户属于多个组，生效的属性值只能有一个，即在应用的Assignments页签下第一个加入的组的相应属性会生效。如果用户所属的组发生变化，则会影响approle的取值。详情请参见Okta用户指南。

验证结果

1. 在Okta左侧导航栏，选择**Applications > Applications**。
2. 单击应用名称role-sso-test。
3. 在**General**页签下的**App Embed Link**区域，获取登录URL。



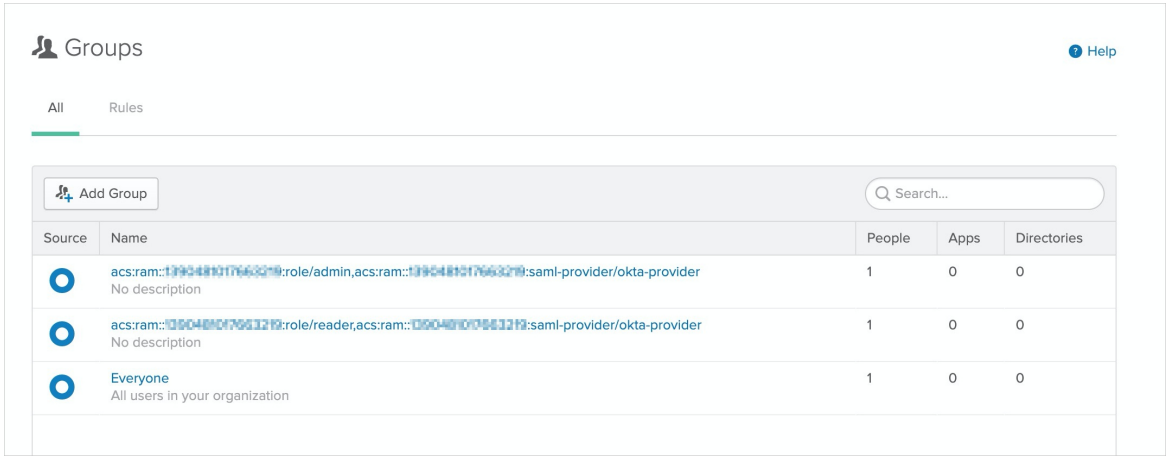
4. 打开另一个浏览器，输入获取到的URL，用username@example.com登录。

   如果成功跳转到您设置的`Default RelayState`对应页面（或默认的阿里云控制台首页），则说明登录成功。

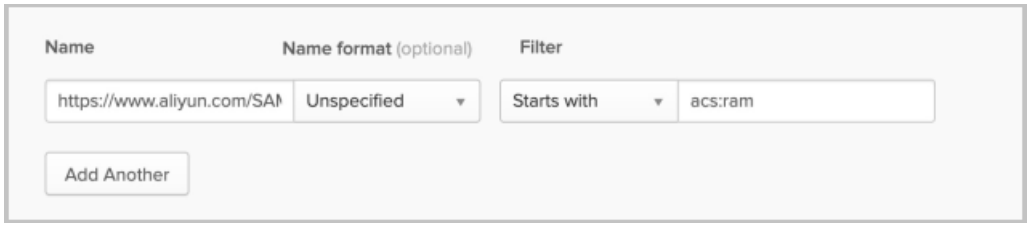
（可选）在Okta中配置用户对应的多个角色

如果您需要让用户对应阿里云的多个角色，则必须使用Group Attribute Statement，借助Group Name进行配置。具体的配置方法如下：

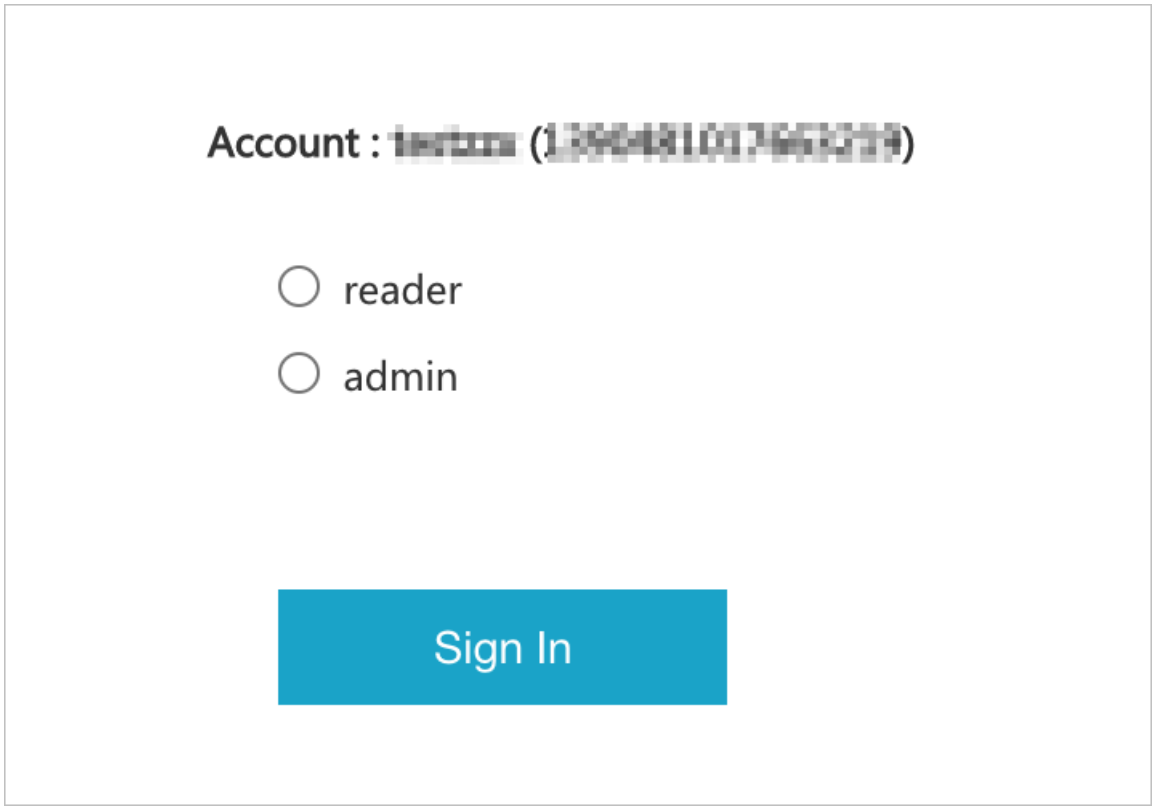
1. 创建多个组。其组名应按照SAML断言中Role Attribute要求的格式，例如：acs:ram::177242285274****:role/admin,acs:ram::177242285274****:saml-provider/okta-provider。



2. 将username@example.com加入多个组。
3. 在应用的**SAML Settings**中，删除Role所对应的attribute statement，然后添加一个Group Attribute Statement。其中，Name填写 `https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName` ，Filter应确保能够过滤出上述组名，例如：Start with acs:ram。



4. 进行上述配置后，再次使用username@example.com登录阿里云时，该用户将会选择登录的角色。



关于Okta的相关操作，请参见Okta用户指南。

4.1.8. 使用Azure AD进行角色SSO的示例

本文提供一个以Azure AD（Azure Active Directory，以下简称 AAD）与阿里云进行角色SSO的示例，帮助用户理解企业IdP与阿里云进行SSO的端到端配置流程。

背景信息

在本示例中，企业拥有一个阿里云账号（Account1）和一个Azure AD租户。在Azure AD租户中，您有一个管理员用户（已授予全局管理员权限）和一个企业员工用户（u2）。您希望经过配置，使得企业员工用户（u2）在登录Azure AD后，通过角色SSO访问阿里云账号（Account1）。

您需要通过管理员用户（已授予全局管理员权限）执行本示例AAD中的操作。关于如何在AAD中创建用户和为用户授权，请参见AAD文档。

步骤一：在AAD库中添加应用程序

1. 管理员用户登录Azure门户。
2. 单击主页的图标。
3. 在左侧导航栏，选择**Azure Active Directory > 企业应用程序 > 所有应用程序**。
4. 单击**新建应用程序**。
5. 搜索**Alibaba Cloud Service (Role-based SSO)**并单击选择。
6. 输入应用名称，然后单击**创建**。

   本示例中，使用默认应用名称 `Alibaba Cloud Service (Role-based SSO)` ，您也可以自定义应用名称。

7. 在Alibaba Cloud Service (Role-based SSO)页面，单击左侧导航栏的**属性**，复制并保存**对象ID**。

步骤二：配置AAD SSO

1. 在Alibaba Cloud Service (Role-based SSO)页面，单击左侧导航栏的**单一登录**。
2. 在**选择单一登录方法**页面，单击SAML。
3. 在**设置SAML单一登录**页面，配置SSO信息。
   i. 在页面左上角，单击**上传元数据文件**，选择文件后，单击**添加**。

      > **说明** 您可以通过以下URL获取元数据文件：`https://signin.alibabacloud.com/saml-role/sp-metadata.xml`。

   ii. 在**基本SAML配置**页面，配置以下信息，然后单击**保存**。
      - **标识符（实体 ID）**：从上一步的元数据文件中自动读取`entityID`的值。
      - **回复 URL（断言使用者服务 URL）**：从上一步的元数据文件中自动读取`Location`的值。
      - **中继状态**：用来配置角色SSO登录成功后跳转到的阿里云页面。

        > **说明** 出于安全原因，您只能填写阿里巴巴旗下的域名URL作为**中继状态**的值，例如：*.aliyun.com、*.hichina.com、*.yunos.com、*.taobao.com、*.tmall.com、*.alibabacloud.com、*.alipay.com，否则配置无效。若不配置，默认跳转到阿里云控制台首页。

   iii. 在**用户属性和声明**区域，单击 图标。

   iv. 单击**添加新的声明**，配置以下信息，然后单击**保存**。
      - 在**名称**区域，输入`Role`。
      - 在**命名空间**区域，输入`https://www.aliyun.com/SAML-Role/Attributes`。
      - 在**源**区域，选择**属性**。
      - 在**源属性**区域，从下拉列表中选择**user.assignedroles**。

   v. 重复上述步骤，添加一个新的声明。
      - 在**名称**区域，输入`RoleSessionName`。
      - 在**命名空间**区域，输入`https://www.aliyun.com/SAML-Role/Attributes`。
      - 在**源**区域，选择**属性**。
      - 在**源属性**区域，从下拉列表中选择**user.userprincipalname**。

   vi. 在**SAML签名证书**区域，单击**下载**，获取**联合元数据XML**。

步骤三：在阿里云创建身份提供商

1. 阿里云账号（Account1）登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，单击SAML页签，然后单击**创建身份提供商**。
4. 在**创建身份提供商**页面，输入**身份提供商名称**`AAD`和**备注**。
5. 在**元数据文档**区域，单击**上传文件**。

> 说明 上传在步骤二：配置AAD SSO中下载的联合元数据XML。

6. 单击**完成**。
7. 单击**关闭**。

步骤四：在阿里云创建RAM角色

1. 在RAM控制台的左侧导航栏，选择**身份管理 > 角色**。
2. 在**角色**页面，单击**创建角色**。
3. 在**创建角色**面板，选择可信实体类型为**身份提供商**，然后单击**下一步**。
4. 输入**角色名称** `AADrole` 和**备注**。
5. 选择身份提供商类型为**SAML**。
6. 在下拉列表中选择身份提供商 `AAD` ，单击**完成**。

> 说明
> - 您可以根据需要为RAM角色添加权限。关于如何为RAM角色添加权限，请参见为RAM角色授权。
> - 当身份提供商和对应的RAM角色创建完成后，请保存好对应的ARN。关于如何查看ARN，请参见查看RAM角色基本信息。

7. 单击**关闭**。

步骤五：将阿里云RAM角色与AAD用户进行关联

1. 在AAD中创建角色。
   i. 管理员用户登录**Azure门户**。
   ii. 在左侧导航栏，选择**Azure Active Directory > 应用注册**。
   iii. 单击**所有应用程序**页签，然后单击**Alibaba Cloud Service (Role-based SSO)**。
   iv. 在左侧导航栏，单击**应用角色**。
   v. 单击**创建应用程序角色**。
   vi. 在**创建应用程序角色**页面，配置以下角色信息，然后单击**应用**。
   - **显示名称**：本示例中输入 `Admin` 。
   - **允许的成员类型**：本示例中选中**用户/组+应用程序**。
   - **值**：输入RAM角色ARN和身份提供商ARN，两者之间用半角逗号（,）分隔。本示例中输入 `acs:ram::187125022722****:role/aadrole,acs:ram::187125022722****:saml-provider/AAD` 。
   - **说明**：输入备注信息。
   - 选中**是否要启用此应用程序角色**。

> 说明 如果您需要在AAD中创建多个角色，请重复上述步骤。

2. 将角色添加到用户（u2）中。
   i. 在左侧导航栏，选择**Azure Active Directory > 企业应用程序 > 所有应用程序**。

ii. 在**名称**列表下，单击Alibaba Cloud Service (Role-based SSO)。

iii. 在左侧导航栏，单击**用户和组**。

iv. 单击左上角的**添加用户/组**。

v. 单击**用户**，从用户列表中选择用户（u2），单击**选择**。

vi. 单击**分配**。

vii. 查看分配的角色。

> **说明** 如果您分配了用户（u2），创建的角色会自动附加给该用户。如果您创建了多个角色，您可以根据需要合理分配角色。

验证结果

1. 获取用户访问URL。

   i. 管理员用户登录Azure门户。

   ii. 在左侧导航栏，选择Azure Active Directory > **企业应用程序** > **所有应用程序**。

   iii. 在**名称**列表下，单击Alibaba Cloud Service (Role-based SSO)。

   iv. 在左侧导航栏，选择**属性**，获取**用户访问URL**。

2. 用户（u2）从管理员用户处获取上述**用户访问URL**，然后在浏览器中输入该URL，使用自己的账号登录。

   系统将自动SSO登录并重定向到您指定的**中继状态**页面。如果未指定**中继状态**或超出允许范围，则系统会访问阿里云控制台首页。

（可选）配置AAD与多个阿里云账号的角色SSO

假设您有两个阿里云账号（Account1和Account2），您希望经过配置，使得企业员工用户（u2）在登录Azure AD后，通过角色SSO既能访问阿里云账号（Account1），也能访问阿里云账号（Account2）。

1. 在AAD库中添加应用程序 `Alibaba Cloud Service (Role-based SSO)` 。

   具体操作，请参见步骤一：在AAD库中添加应用程序。

2. 配置AAD SSO。

   具体操作，请参见步骤二：配置AAD SSO。

3. 在阿里云创建身份提供商。

   您需要在两个阿里云账号（Account1和Account2）中分别创建身份提供商 `AAD` 。

   每个阿里云账号内的具体操作，请参见步骤三：在阿里云创建身份提供商。

4. 在阿里云创建RAM角色。

   您需要在两个阿里云账号（Account1和Account2）中分别创建RAM角色，本示例中假设在阿里云账号（Account1）中创建两个RAM角色，在阿里云账号（Account2）中创建一个RAM角色。具体如下：

   - 阿里云账号（Account1）的RAM角色： `adminaad` 和 `readaad` 。
   - 阿里云账号（Account2）的RAM角色： `financeaad` 。

   每个阿里云账号内的具体操作，请参见步骤四：在阿里云创建RAM角色。

5. 将阿里云RAM角色与AAD用户（u2）进行关联。

   在AAD中创建三个角色，将三个角色添加到用户（u2）中。三个角色的值分别为：

   - `acs:ram::<Account1_ID>:role/adminaad,acs:ram::<Account1_ID>:saml-provider/AAD`
   - `acs:ram::<Account1_ID>:role/readaad,acs:ram::<Account1_ID>:saml-provider/AAD`
   - `acs:ram::<Account2_ID>:role/financeaad,acs:ram::<Account2_ID>:saml-provider/AAD`

   具体操作，请参见步骤五：将阿里云RAM角色与AAD用户进行关联。

6. AAD用户（u2）通过角色SSO访问阿里云。

   用户（u2）登录Azure的我的应用页面，单击应用程序Alibaba Cloud Service (Role-based SSO)。然后在阿里云界面上，您需要根据提示选择要访问的阿里云账号（Account1或Account2）及其角色，从而以角色SSO方式访问阿里云。

4.1.9. 使用OneLogin进行角色SSO的示例

本文提供一个以OneLogin与阿里云进行角色SSO的示例，帮助您理解企业IdP与阿里云进行角色SSO的端到端配置流程。

背景信息

本示例中，企业拥有一个阿里云账号、一个OneLogin管理员用户和多个OneLogin普通用户。您希望经过配置，使OneLogin普通用户直接使用OneLogin账号通过角色SSO的方式访问阿里云，而不是在阿里云重新创建账号。

关于什么是OneLogin，请参见OneLogin帮助文档。

步骤一：在OneLogin创建应用

1. 使用管理员用户登录OneLogin。
2. 在账号头像的左侧，单击Administration，进入管理员页面。
3. 在顶部菜单栏，选择Applications > Applications。
4. 在Applications页面的右上角，单击Add App。
5. 在Find Applications页面，搜索SAML Test Connector (Advanced)。
6. 在Add SAML Test Connector (Advanced)页面，配置应用程序的基本信息，然后单击Save。

本示例中设置应用程序的Display Name为 `LoginToAliyun` ，其他参数保持默认值。

7. 在Info页面，鼠标悬浮在右上角的More Actions上，从下拉列表中单击SAML Metadata，下载身份提供商（IdP）元数据文件，并将其保存在本地计算机上。

步骤二：在阿里云创建身份提供商

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，单击SAML页签，然后单击**创建身份提供商**。
4. 在**创建身份提供商**页面，输入**身份提供商名称**（OneLogin）和**备注**。
5. 在**元数据文档**区域，单击**上传文件**，上传从步骤一：在OneLogin创建应用获取的IdP元数据。
6. 单击**完成**。
7. 单击**关闭**。

   查看新创建的身份提供商详情，记录其ARN，方便您后续使用。

步骤三：在阿里云创建RAM角色

1. 在RAM控制台的左侧导航栏，选择**身份管理 > 角色**。
2. 在**角色**页面，单击**创建角色**。
3. 在**创建角色**面板，选择可信实体类型为**身份提供商**，单击**下一步**。
4. 输入**角色名称**（例如：Reader-OneLogin）和**备注**。
5. 选择身份提供商类型为SAML。
6. 选择从步骤二：在阿里云创建身份提供商中创建的身份提供商（OneLogin）并查看限制条件后，单击**完成**。
7. 单击**关闭**。

   查看新创建的RAM角色详情，记录其ARN，方便您后续使用。

步骤四：在OneLogin配置应用

1. 使用管理员用户登录OneLogin。
2. 创建自定义用户属性。
   i. 在顶部菜单栏，选择Users > Users。
   ii. 在Users页面，鼠标悬浮在右上角的More Actions上，从下拉列表中单击Custom user fields。
   iii. 在Custom User Fields页面的右上角，单击New User Field。
   iv. 在New User Field对话框，配置Name和Shortname，然后单击Save。

   本示例中，Name设置为 `AliyunRoles for SSO` ，Shortname设置为 `AliyunRoles` 。
3. 配置应用。
   i. 在顶部菜单栏，选择Applications > Applications。
   ii. 在Applications页面，单击步骤一：在OneLogin创建应用创建的应用程序（LoginToAliyun）。
   iii. 在左侧导航栏，单击Configuration。

iv. 在Configuration页面，配置以下信息，然后单击Save。

- RelayState：用来配置用户登录成功后跳转到的阿里云页面。

  > **说明** 出于安全原因，您只能填写阿里巴巴旗下的域名URL作为RelayState的值，例如：*.aliyun.com、*.hichina.com、*.yunos.com、*.taobao.com、*.tmall.com、*.alibabacloud.com、*.alipay.com，否则配置无效。若不配置，默认跳转到阿里云控制台首页。

- Audience (EntityID)：`urn:alibaba:cloudcomputing:international`。
- Recipient：`https://signin.alibabacloud.com/saml-role/sso`。
- ACS (Consumer) URL：`https://signin.alibabacloud.com/saml-role/sso`。

v. 在左侧导航栏，单击Parameters。

vi. 在Parameters页面，单击＋，添加第一条自定义应用属性。

a. 在New Field对话框，设置Field name为`https://www.aliyun.com/SAML-Role/Attributes/Role`，然后选中Include in SAML assertion和Multi-value parameter，最后单击Save。

b. 在Edit Field https://www.aliyun.com/SAML-Role/Attributes/Role对话框，从Default if no value selected区域的两个下拉列表中分别选择Aliyun Roles for SSO (Custom)和Semicolon Delimited input (Multi-value output)，然后单击Save。

vii. 在Parameters页面，单击＋，添加第二条自定义应用属性。

a. 在New Field对话框，设置Field name为`https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName`，然后选中Include in SAML assertion，最后单击Save。

b. 在Edit Field https://www.aliyun.com/SAML-Role/Attributes/RoleSessionName对话框，从Value区域的下拉列表中选择Email，然后单击Save。

> **说明** 您也可以根据实际需要设置Value为其他值，例如：Username、userPrincipalName等。

viii. 在Parameters页面的右上角，单击Save。

步骤五：在OneLogin创建用户并分配应用

1. 使用管理员用户登录OneLogin。
2. 在顶部菜单栏，选择Users > Users。
3. 创建用户。

> **说明** 如果您已经拥有OneLogin用户，请跳过此步。

i. 在Users页面的右上角，单击New User。

ii. 在New User页面，设置First name（例如：Jack）、Last name（例如：Lee）、Username（例如：jacklee）Email（例如：jacklee@example.com），然后单击Save User。

iii. 在User Info页面，鼠标悬浮在右上角的More Actions上，从下拉列表中单击Change Password，为用户设置登录密码，然后单击Update。

为用户设置登录密码，以保证其可以正常登录到OneLogin。

4. 在User Info页面的Custom Fields区域，配置用户自定义属性Aliyun Roles for SSO的值。

Aliyun Roles for SSO取值由RAM角色ARN和身份供应商ARN组成，两者之间用半角逗号（,）分隔，具体格式为 `acs:ram::<account_id>:role/RoleName,acs:ram::<account_id>:saml-provider/ProviderName` 。其中，RAM角色ARN从步骤三：在阿里云创建RAM角色获取，身份供应商ARN从步骤二：在阿里云创建身份提供商获取，<account_id>为阿里云账号ID。

> 说明 如果一个用户对应多个RAM角色，此处可配置多组值。每个RAM角色ARN和其对应的身份提供商ARN为一组值，多组值之间用半角分号（;）分隔。例如： `acs:ram::125022144354****:role/reader-onelogin,acs:ram::125022144354****:saml-provider/OneLogin;acs:ram::125022144354****:role/administrator-onelogin,acs:ram::125022144354****:saml-provider/OneLogin;acs:ram::158622887609****:role/finance,acs:ram::158622887609****:saml-provider/OneLogin2` 。

5. 为用户分配应用。

i. 在Applications页面，单击 ⊕ 。

ii. 选择步骤一：在OneLogin创建应用创建的应用（LoginToAliyun），然后单击Continue。

iii. 在弹出的对话框中，单击Save。

6. 在Users页面的右上角，单击右上角的Save User。
7. 重复步骤~，为其他OneLogin普通用户配置Aliyun Roles for SSO属性值并分配应用。

结果验证

1. 使用步骤五：在OneLogin创建用户并分配应用创建的用户（jacklee）登录OneLogin。
2. 单击应用（LoginToAliyun）。

如果成功跳转到您设置的RelayState对应页面（或默认的阿里云控制台首页），则说明登录成功。

> 说明 如果您在步骤五：在OneLogin创建用户并分配应用中为用户设置了多个角色，则需要先选择登录角色，才能访问阿里云。

4.2. 基于OIDC的角色SSO

4.2.1. OIDC角色SSO概览

OIDC（OpenID Connect）是建立在OAuth 2.0基础上的一个认证协议，阿里云RAM支持基于OIDC的角色SSO。

基本概念

概念	说明

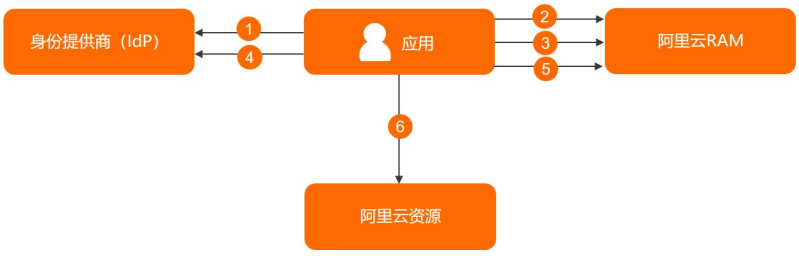
概念	说明
OIDC	OIDC（OpenID Connect）是建立在OAuth 2.0基础上的一个认证协议。OAuth是授权协议，而OIDC在OAuth协议上构建了一层身份层，除了OAuth提供的授权能力，它还允许客户端能够验证终端用户的身份，以及通过OIDC协议的API（HTTP RESTful形式）获取用户的基本信息。
OIDC令牌	OIDC可以给应用签发代表登录用户的身份令牌，即OIDC令牌（OIDC Token）。OIDC令牌用于获取登录用户的基本信息。
临时身份凭证	STS（Security Token Service）是阿里云提供的一种临时访问权限管理服务，通过STS获取可以自定义时效和访问权限的临时身份凭证（STS Token）。
颁发者URL	颁发者URL由外部IdP提供，对应OIDC Token中的 `iss` 字段值。颁发者URL必须以 `https` 开头，符合标准URL格式，但不允许带有query参数（以 `?` 标识）、fragment片段（以 `#` 标识）和登录信息（以 `@` 标识）。
验证指纹	为了防止颁发者URL被恶意劫持或篡改，您需要配置外部IdP的HTTPS CA证书生成的验证指纹。阿里云会辅助您自动计算该验证指纹，但是建议您在本地自己计算一次（例如：使用OpenSSL计算指纹），与阿里云计算的指纹进行对比。如果对比发现不同，则说明该颁发者URL可能已经受到攻击，请您务必再次确认，并填写正确的指纹。
客户端ID	您的应用在外部IdP注册的时候，会生成一个客户端ID（Client ID）。当您从外部IdP申请签发OIDC令牌时必须使用该客户端ID，签发出来的OIDC令牌也会通过 `aud` 字段携带该客户端ID。在创建OIDC身份提供商时配置该客户端ID，然后在使用OIDC令牌换取STS Token时，阿里云会校验OIDC令牌中 `aud` 字段所携带的客户端ID与OIDC身份提供商中配置的客户端ID是否一致。只有一致时，才允许扮演角色。

应用场景

当企业应用需要频繁访问阿里云时，如果使用固定的访问密钥（AccessKey），且安全防护措施不足时，可能会因AccessKey泄露而带来安全隐患。为了解决这个问题，有些企业会将应用注册在企业自建或者第三方的具有OIDC能力的身份提供商中（例如：Google G Suite或Okta等），以借助OIDC身份提供商的能力来为应用生成OIDC令牌（OIDC Token）。在这种情况下，借助阿里云RAM提供的角色SSO能力，企业应用可以通过持有的OIDC令牌换取阿里云临时身份凭证（STS Token），从而安全地访问阿里云资源。

此外，有些个人开发者或中小企业允许员工使用其在一些网站（例如：社交网站）上注册的身份来登录阿里云，如果这些网站支持生成OIDC令牌，则可以使用阿里云RAM来完成基于OIDC的单点登录。

基本流程



1. 在外部IdP中注册应用，获取应用的客户端ID（Client ID）。
2. 在阿里云RAM中创建OIDC身份提供商，配置阿里云与外部IdP的信任关系。

   具体操作，请参见创建OIDC身份提供商。
3. 在阿里云RAM中创建可信实体为OIDC身份提供商的RAM角色，并为RAM角色授权。

具体操作，请参见创建OIDC身份提供商的RAM角色和为RAM角色授权。

4. 在外部IdP中签发OIDC令牌（OIDC Token）。

   具体操作，请参见外部IdP的对应文档。

5. 使用OIDC Token换取STS Token。

   具体操作，请参见AssumeRoleWithOIDC。

6. 使用STS Token访问阿里云资源。

配置示例

使用OIDC进行角色SSO的示例

使用限制

限制项	最大值
一个阿里云账号中可创建的OIDC身份提供商个数	100
一个OIDC身份提供商中的客户端ID个数	20
一个OIDC身份提供商中的验证指纹个数	5

4.2.2. 管理OIDC身份提供商

在使用OIDC角色SSO时，需要创建身份提供商。

创建OIDC身份提供商

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**OIDC**页签，然后单击**创建身份提供商**。
4. 在**创建身份提供商**页面，设置身份提供商信息。

参数	说明
身份提供商名称	同一个阿里云账号下必须唯一。
颁发者URL	颁发者URL由外部IdP提供。颁发者URL必须以 `https` 开头，符合标准URL格式，但不允许带有query参数（以 `?` 标识）、fragment片段（以 `#` 标识）和登录信息（以 `@` 标识）。
验证指纹	为了防止颁发者URL被恶意劫持或篡改，您需要配置外部IdP的HTTPS CA证书生成的验证指纹。阿里云会辅助您自动计算该验证指纹，但是建议您在本地自己计算一次（例如：使用OpenSSL计算指纹），与阿里云计算的指纹进行对比。如果对比发现不同，则说明该颁发者URL可能已经受到攻击，请您务必再次确认，并填写正确的指纹。

参数	说明
客户端ID	您的应用在外部IdP注册的时候，会生成一个客户端ID（Client ID）。当您从外部IdP申请签发OIDC令牌时必须使用该客户端ID，签发出来的OIDC令牌也会通过 `aud` 字段携带该客户端ID。在创建OIDC身份提供商时配置该客户端ID，然后在使用OIDC令牌换取STS Token时，阿里云会校验OIDC令牌中 `aud` 字段所携带的客户端ID与OIDC身份提供商中配置的客户端ID是否一致。只有一致时，才允许扮演角色。 如果您有多个应用需要访问阿里云，您可以配置多个客户端ID，但最多不能超过20个。
备注	身份提供商的描述信息。

5. 单击**确定**。

查看OIDC身份提供商信息

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**OIDC**页签，然后单击目标身份提供商名称。
4. 在**身份提供商信息**区域，查看**身份提供商名称**、**身份提供商类型**、**创建时间**、**更新时间**、**备注**、**ARN**和**颁发者URL**。

修改OIDC身份提供商信息

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**OIDC**页签，然后单击目标身份提供商名称。
4. 在**身份提供商信息**区域，单击**备注**右侧的**编辑**，修改备注信息。
5. 在**客户端ID**区域，单击**添加**或**删除**，添加或删除客户端ID。

> **说明** 最多添加20个客户端ID。只有1个客户端ID时，无法删除。

6. 在**指纹**区域，单击**添加**或**删除**，添加或删除验证指纹。

> **说明** 最多添加5个验证指纹。只有1个验证指纹时，无法删除。

删除OIDC身份提供商

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**OIDC**页签，然后单击目标OIDC身份提供商**操作**列的**删除**。
4. 在**删除身份提供商**对话框，单击**确定**。

4.2.3. 使用OIDC进行角色SSO的示例

本文提供一个Okta与阿里云进行OIDC角色SSO的示例，使Okta中的应用通过临时身份凭证（STS Token）安全访问阿里云资源。

前提条件

请提前在Okta中注册一个OIDC应用，并获取应用的颁发者URL和客户端ID（Client ID）。本示例中使用的数据如下：

- 颁发者URL：https://dev-xxxxxx.okta.com
- 客户端ID：0oa294vi1vJoClev****

步骤一：在阿里云创建OIDC身份提供商

本步骤中将创建一个名为 `TestOidcProvider` 的OIDC身份提供商。**颁发者URL**为 `https://dev-xxxxxx.okta.com` ，**客户端ID**为 `0oa294vi1vJoClev****` 。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，单击**SSO管理**。
3. 在**角色SSO**页签，先单击**OIDC**页签，然后单击**创建身份提供商**。
4. 在**创建身份提供商**页面，设置身份提供商信息。

参数	说明
身份提供商名称	同一个阿里云账号下必须唯一。
颁发者URL	颁发者URL由外部IdP提供。颁发者URL必须以 `https` 开头，符合标准URL格式，但不允许带有query参数（以 `?` 标识）、fragment片段（以 `#` 标识）和登录信息（以 `@` 标识）。
验证指纹	为了防止颁发者URL被恶意劫持或篡改，您需要配置外部IdP的HTTPS CA证书生成的验证指纹。阿里云会辅助您自动计算该验证指纹，但是建议您在本地自己计算一次（例如：使用OpenSSL计算指纹），与阿里云计算的指纹进行对比。如果对比发现不同，则说明该颁发者URL可能已经受到攻击，请您务必再次确认，并填写正确的指纹。
客户端ID	您的应用在外部IdP注册的时候，会生成一个客户端ID（Client ID）。当您从外部IdP申请签发OIDC令牌时必须使用该客户端ID，签发出来的OIDC令牌也会通过 `aud` 字段携带该客户端ID。在创建OIDC身份提供商时配置该客户端ID，然后在使用OIDC令牌换取STS Token时，阿里云会校验OIDC令牌中 `aud` 字段所携带的客户端ID与OIDC身份提供商中配置的客户端ID是否一致。只有一致时，才允许扮演角色。 如果您有多个应用需要访问阿里云，您可以配置多个客户端ID，但最多不能超过20个。
备注	身份提供商的描述信息。

5. 单击**确定**。

步骤二：在阿里云创建可信实体为OIDC身份提供商的RAM角色

本步骤中将创建一个名为 `testoidc` 的RAM角色，身份提供商选择步骤一创建的 `TestOidcProvider` 。

1. 使用阿里云账号登录RAM控制台。

2. 在左侧导航栏，选择**身份管理 > 角色**。
3. 在**角色**页面，单击**创建角色**。
4. 在**创建角色**面板，选择可信实体类型为**身份提供商**，然后单击**下一步**。
5. 输入**角色名称**和**备注**。
6. 选择身份提供商类型为**OIDC**。
7. 选择身份提供商并设置限制条件，然后单击**完成**。

   支持的限制条件如下表所示：

限制条件关键字	说明	是否必选	示例
oidc:iss	OIDC颁发者（Issuer）。用来扮演角色的OIDC令牌中的iss字段值必须满足该限制条件要求，角色才允许被扮演。 该限定条件必须使用StringEquals作为条件操作类型，条件值只能是您在OIDC身份提供商中填写的颁发者URL。该限制条件用于确保只有受信颁发者颁发的OIDC令牌才能扮演角色。	是	https://dev-xxxxxx.okta.com
oidc:aud	OIDC受众（Audience）。用来扮演角色的OIDC令牌中的aud字段值必须满足该限制条件要求，角色才允许被扮演。 该限定条件必须使用StringEquals作为条件操作类型，您可选择在OIDC身份提供商中配置的一个或多个客户端ID（Client ID）作为条件值。该限制条件用于确保只有您设置的Client ID生成的OIDC令牌才能扮演角色。	是	0oa294vi1vJoClev****
oidc:sub	OIDC主体（Subject）。用来扮演角色的OIDC令牌中的sub字段值必须满足该限制条件要求时，角色才允许被扮演。 该限定条件可以使用任何String类的条件操作类型，且您可以最多设置10个OIDC主体作为条件值。该限制条件用于进一步限制允许扮演角色的身份主体，您也可以不指定该限制条件。	否	00u294e3mzNXt4Hi****

8. 单击**关闭**。

步骤三：为RAM角色授权

您可以根据实际需要，为步骤二创建的RAM角色 `testoidc` 授予访问阿里云资源的权限。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**身份管理 > 角色**。
3. 在**角色**页面，单击目标RAM角色**操作**列的**添加权限**。
4. 在**添加权限**面板，为RAM角色添加权限。

i. 选择授权应用范围。

- **整个云账号**：权限在当前阿里云账号内生效。
- **指定资源组**：权限在指定的资源组内生效。

> **说明** 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见支持资源组的云服务。

ii. 输入授权主体。

授权主体即需要授权的RAM角色，系统会自动填入当前的RAM角色，您也可以添加其他RAM角色。

iii. 选择权限策略。

> **说明** 每次最多绑定5条策略，如需绑定更多策略，请分次操作。

5. 单击**确定**。
6. 单击**完成**。

步骤四：在Okta签发OIDC令牌（OIDC Token）

阿里云不支持使用OIDC登录控制台，所以您需要使用程序访问的方式完成OIDC SSO流程。由于生成OIDC Token本质上是个OAuth流程，所以您需要通过标准的OAuth 2.0流程从OIDC IdP（例如：Okta）获取OIDC Token。OAuth支持多种流程，例如：比较常见的Authorization Code Flow。但由于该流程较为复杂，为演示方便，如下将以比较简单的Implicit Flow为例，为您介绍获取OIDC Token并最终完成SSO的流程，其中简化了标准协议要求的部分步骤。

1. 搭建一个客户端Web应用，用于接收Okta颁发的OIDC Token。

   本示例中，将提供一个使用Java Spring Boot和Thymeleaf搭建的极简客户端Web应用。在本机8080端口部署Web应用，绑定的localhost指向127.0.0.1，因此在本机通过浏览器访问localhost:8080就可以访问到该Web应用。相关的示例代码如下：

   - 静态页面示例代码

     按照OAuth 2.0协议要求Okta回调给客户端Web应用的信息是通过锚点（fragment）来传递的，您可以通过一个Web页面，直接提取出锚点参数来获取回调的OIDC Token。假设您制作了如下这个简单的静态页面，直接进行参数透传。该页面的完整地址为 `http://localhost:8080/accessTokenCallback` ，也就是Okta应用配置的回调地址 `redirect_uri` 。

```
<!DOCTYPE HTML>
<html xmlns:th="http://www.thymeleaf.org">
    <head>
        <script>
            window.onload = function () {
                let fragment = window.location.hash.substring(1);
                window.location.href = "/receiveAccessToken?" + fragment;
            };
        </script>
    </head>
</html>
```

   - 类示例代码

     创建一个类，作为上述静态页面的控制器。

```
package com.aliyun.oauthtest;
import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.RequestMapping;
@Controller
public class CallbackController {
    @RequestMapping("accessTokenCallback")
    public String callback() {
        return "accessTokenCallback";
    }
}
```

2. 登录Okta，向Okta申请签发OIDC Token。

   您需要先登录Okta，然后基于步骤1搭建的客户端Web应用，直接构造并访问URL：`https://dev-xxxxxx.okta.com/oauth2/v1/authorize?client_id=0oa294vi1vJoClev****&scope=openid&response_type=token%20id_token&state=testState&nonce=a_unique_nonce_1&redirect_uri=http%3A%2F%2Flocalhost%3A8080%2FaccessTokenCallback`

   参数含义如下：

   - `client_id`：Okta中注册的OIDC应用的客户端ID。
   - `scope`：取值为`openid`。
   - `response_type`：Implicit Flow流程中取值为`token id_token`。
   - `state`：表示客户端的当前状态，可以指定任意值。
   - `nonce`：防止重放攻击，可以指定任意值。
   - `redirect_uri`：接收`access_token`或`id_token`的回调地址，即步骤1中的客户端Web应用的地址。

   本示例中已经预先登录了Okta，所以系统会根据用户设置的`redirect_uri`重定向到回调地址。如下地址中的`id_token`就是OIDC Token。

   ```
   HTTP/1.1 302 Found
   Location:  http://localhost:8080/accessTokenCallback#id_token=eyJraWQiOiJ6OUV0e****&access_token=eyJraWQiOiJseEQ3R****&token_type=Bearer&expires_in=3600&scope=openid&state=testState
   ```

3. 解析OIDC Token。

   您可以对步骤2获取的结果进行简单地解析，将`header`和`payload`展开。

   请求示例：

```
package com.aliyun.oauthtest;
import java.util.Base64;
import java.util.Base64.Decoder;
import java.util.HashMap;
import java.util.Map;
import java.util.TreeMap;
import com.alibaba.fastjson.JSON;
import com.alibaba.fastjson.JSONObject;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.RequestMethod;
import org.springframework.web.bind.annotation.RequestParam;
import org.springframework.web.bind.annotation.RestController;
@RestController
public class ClientAppController {
    @RequestMapping(value = "/receiveAccessToken", method = {RequestMethod.POST, Reques
tMethod.GET},
            produces = "application/json")
    public Map<String, Object> receiveAccessToken(@RequestParam("access_token") String
accessToken,
                                                  @RequestParam("id_token") String idTo
ken,
                                                  @RequestParam("token_type") String to
kenType,
                                                  @RequestParam("expires_in") Long expi
reTime,
                                                  @RequestParam("scope") String scope,
                                                  @RequestParam("state") String state)
    {
        Map<String, Object> result = new TreeMap<>();
        result.put("access_token", accessToken);
        result.put("id_token", idToken);
        result.put("token_type", tokenType);
        result.put("expires_in", "" + expireTime);
        result.put("scope", scope);
        result.put("state", state);
        String[] jwt = idToken.split("\\.");
        Decoder decoder = Base64.getDecoder();
        result.put(" id token jwt header", JSON.parse(new String(decoder.decode(jwt[0])
)));
        result.put(" id token jwt payload", JSON.parse(new String(decoder.decode(jwt[1]
))));
        result.put(" id token jwt signature", jwt[2]);
        return result;
    }
}
```

返回示例：

```
{
    " id token jwt header": {
        "kid": "z9EtyT345d-JLIJo2-5ySDO27LG4FPeOotbwJPT****",
        "alg": "RS256"
    },
    " id token jwt payload": {
        "at_hash": "KKsdN3prZWTvBEMn-g****",
        "sub": "00u294e3mzNXt4Hi****",
        "aud": "0oa294vi1vJoClev****",
        "ver": 1,
        "idp": "0oa294iehxjUCZIO****",
        "amr": [
            "pwd"
        ],
        "auth_time": 1636373097,
        "iss": "https://dev-xxxxxx.okta.com",
        "exp": 1636377759,
        "iat": 1636374159,
        "nonce": "a_unique_nonce_1",
        "jti": "ID.lmSU5AD2iKLCVu6_KLMIr52dpCprncxW38v-NCA****"
    },
    "id token jwt signature": "ZEJEGIv4Zoau63****",
    "access_token": "eyJraWQiOiJseEQ3R****",
    "expires_in": "3600",
    "id_token": "eyJraWQiOiJ6OUV0e****",
    "scope": "openid",
    "state": "testState",
    "token_type": "Bearer"
}
```


步骤五：使用OIDC Token换取STS Token

您可以直接调用AssumeRoleWithOIDC API，使用从步骤四获取的未解析的OIDC Token换取STS Token。

请求示例：

```
public static void main(String[] args)
{
    IAcsClient client = initialization();
    String jwtToken = "eyJraWQiOiJ6OUV0e****"; //从Okta获取的未解析的id_token。
    AssumeRoleWithOIDCRequest request = new AssumeRoleWithOIDCRequest();
    request.setDurationSeconds(3600L);
    request.setOIDCProviderArn("acs:ram::113511544585****:oidc-provider/TestOidcProvider");
    request.setOIDCToken(jwtToken);
    request.setRoleArn("acs:ram::113511544585****:role/testoidc");
    request.setRoleSessionName("TestOidcAssumedRoleSession");
    try
    {
        AssumeRoleWithOIDCResponse resp = client.getAcsResponse(request);
        System.out.println("success requestId: " + resp.getRequestId());
        System.out.println("success assume role arn: " + resp.getAssumedRoleUser().getArn()
);
        System.out.println("success sts credential accessKey id: " + resp.getCredentials().
getAccessKeyId());
        System.out.println("success sts credential accessKey secret: " + resp.getCredential
s().getAccessKeySecret());
        System.out.println("success resp: " + JSON.toJSONString(resp));
    }
    catch(ClientException | SystemException e)
    {
        e.printStackTrace();
    }
}
```

返回示例：

```
success requestId: 3D57EAD2-8723-1F26-B69C-F8707D8B565D
success assume role arn: acs:ram::113511544585****:role/testoidc/TestOidcAssumedRoleSession
success sts credential accessKey id: STS.NUgYrLnoC37mZZCNnAbez****
success sts credential accessKey secret: CVwjCkNzTMupZ8NbTCxCBRq3K16jtcWFTJAyBEv2****
success resp:
{
    "AssumedRoleUser":
    {
        "Arn": "acs:ram::113511544585****:role/testoidc/TestOidcAssumedRoleSession",
        "AssumedRoleId": "33157794895460****:TestOidcAssumedRoleSession"
    },
    "Credentials":
    {
        "AccessKeyId": "STS.NUgYrLnoC37mZZCNnAbez****",
        "AccessKeySecret": "CVwjCkNzTMupZ8NbTCxCBRq3K16jtcWFTJAyBEv2****",
        "Expiration": "2021-10-20T04:27:09Z",
        "SecurityToken": "CAIShwJ1q6Ft5B2yfSjIr****"
    },
    "OIDCTokenInfo":
    {
        "ClientIds": "0oa294vi1vJoClev****",
        "Issuer": "https://dev-xxxxxx.okta.com",
        "Subject": "00u294e3mzNXt4Hi****"
    },
    "RequestId": "3D57EAD2-8723-1F26-B69C-F8707D8B565D"
}
```

其中 `Credentials` 中的信息即为STS Token。

步骤六：使用STS Token访问阿里云资源

使用从步骤五获取的STS Token访问有权限的阿里云资源。