阿里云
访问控制

单点登录管理（SSO）

文档版本：20190920

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 SSO概览

阿里云支持基于SAML 2.0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

阿里云提供基于SAML 2.0协议的SSO。为了更好的理解SSO，下面简要介绍与SAML / SSO相关的一些基本概念：

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。

SSO的方式

企业根据自身需要，使用支持SAML 2.0的企业IdP（例如：AD FS）与阿里云进行SSO。阿里云提供以下两种基于SAML 2.0协议的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。请参见#unique_4。

- 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。请参见#unique_5。

SSO方式的比较

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	一个IdP关联多个阿里云账号	多个IdP
用户SSO	√	√	×	×	×
角色SSO	×	√	√	√	√

说明：

- “√”支持，“×”表示不支持。
- 关于用户SSO与角色SSO的更多比较，请参见#unique_6。

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#unique_8。
- 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

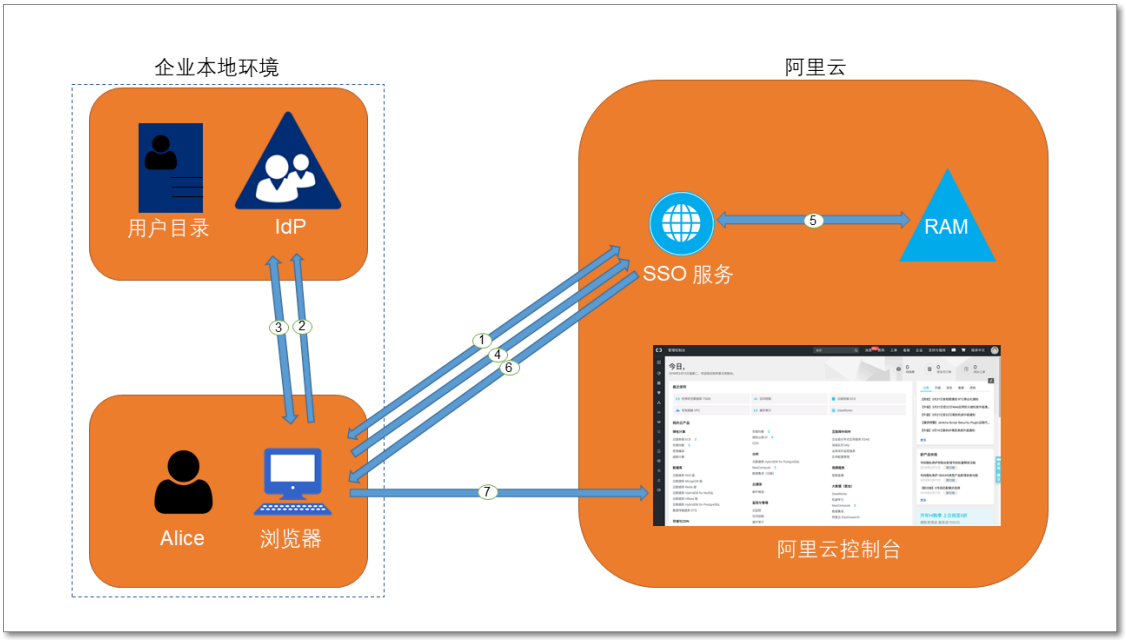
3.1 进行用户SSO

本文为您介绍用户SSO的背景、基本流程以及配置步骤。

背景信息

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用户身份访问阿里云。

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用户身份。
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1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的登录页直接点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。

   详情请参见阿里云用户SSO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。

   详情请参见进行用户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。

   详情请参见#unique_13。

后续步骤

由于不同IdP的系统差异，关于SAML SP配置和断言属性配置的操作流程都有些差异。我们会提供一个以AD FS（Microsoft Active Directory Federation Service）与阿里云进行用户SSO的示例，用于帮助理解企业IdP与阿里云的端到端配置流程。

详情请参见#unique_14。

3.2 阿里云用户SSO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。

前提条件

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#unique_15和#unique_16。

操作步骤

1. 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：
   该功能只对云账号下的所有RAM用户生效，不会影响云账号的登录。

   - 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，请参见进行用户SSO时企业IdP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或默认域名作为后缀。

后续步骤

完成SAML配置后，选择以下一种方法，将企业IdP中的用户数据迁移或同步到阿里云RAM：

· 登录RAM控制台手动创建与企业IdP匹配的RAM用户。
· 使用RAM SDK编写程序或基于阿里云CLI来定制解决方案。

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。
   a) 云账号登录RAM控制台。
   b) 在左侧导航栏，单击SSO管理。
   c) 单击用户SSO。
   d) 在SSO登录设置区域，可以查看当前云账号的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：
   - 直接使用上述阿里云的元数据URL进行配置。
   - 如果您的IdP不支持URL配置，您可以根据上述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：
       您只能填写`*.console.aliyun.com`域名下的URL作为`RelayState`的值。

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。

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#unique_16。
- 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_alias>为辅助域名。关于如何设置辅助域名，请参见设置辅助域名。

  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#unique_18。

  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。

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：example2.com，SAML断言中的NameID取值为：Alice@example.onaliyun.com或Alice@example2.com。
- 如果设置了域别名为：example.com后，又设置了辅助域名为：example2.com，SAML断言中的NameID取值为：Alice@example.onaliyun.com或Alice@example.com。

3.4 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 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。

注意事项

本文以 Windows Server 2012 R2 为例，介绍如何配置 AD FS 与阿里云，从而实现 SSO。

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 的端到端配置，阿里云不提供 Microsoft Active Directory 配置官方咨询服务。

前提条件

用户对 Microsoft Active Directory (AD) 需进行合理正确的配置，在 Windows Server 2012 R2 上配置以下服务器角色：

- 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。

示例配置

示例中用到的相关配置如下：

- 云账号的默认域名为：`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 服务名称为：`adfs.secloud.club`。
- 创建的 Microsoft AD 的域名为：`secloud.club`，NETBIOS 名为：`secloud`。
- RAM 用户 `alice` 在 AD 中的 UPN 为：`alice@secloud.club`，域内登录也可以使用：`secloud\alice`。

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
```

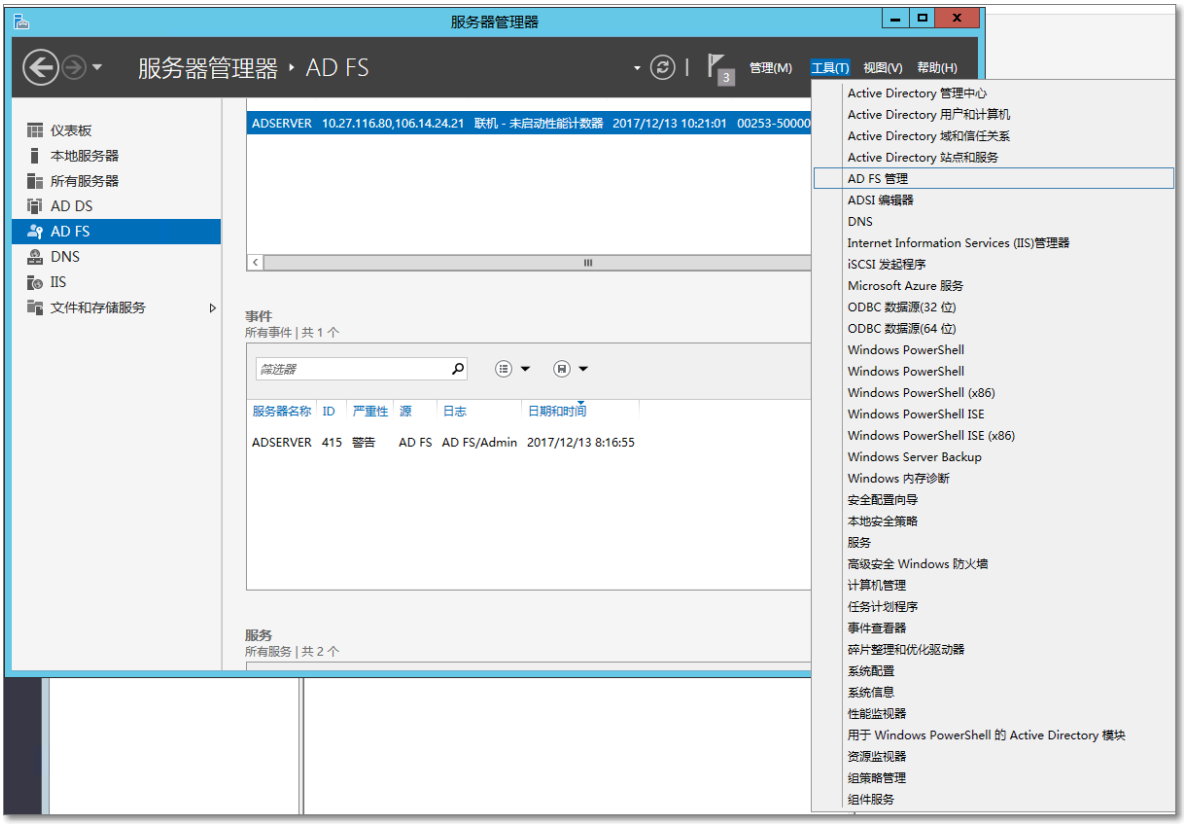
2. 将元数据 XML 文件下载到本地。
3. 在 RAM 控制台的 SSO 配置时使用下载好的元数据文件。

具体配置请参考：#unique_17。

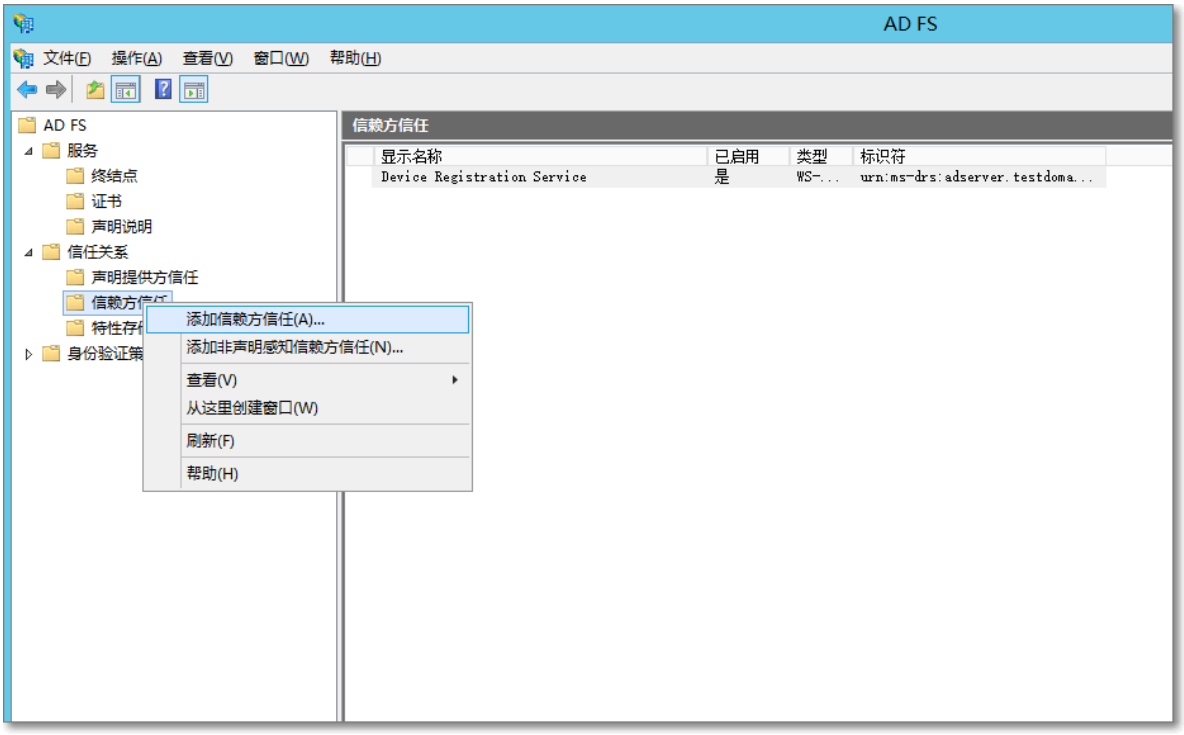
在 AD FS 中将阿里云配置为可信 SAML SP

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 。

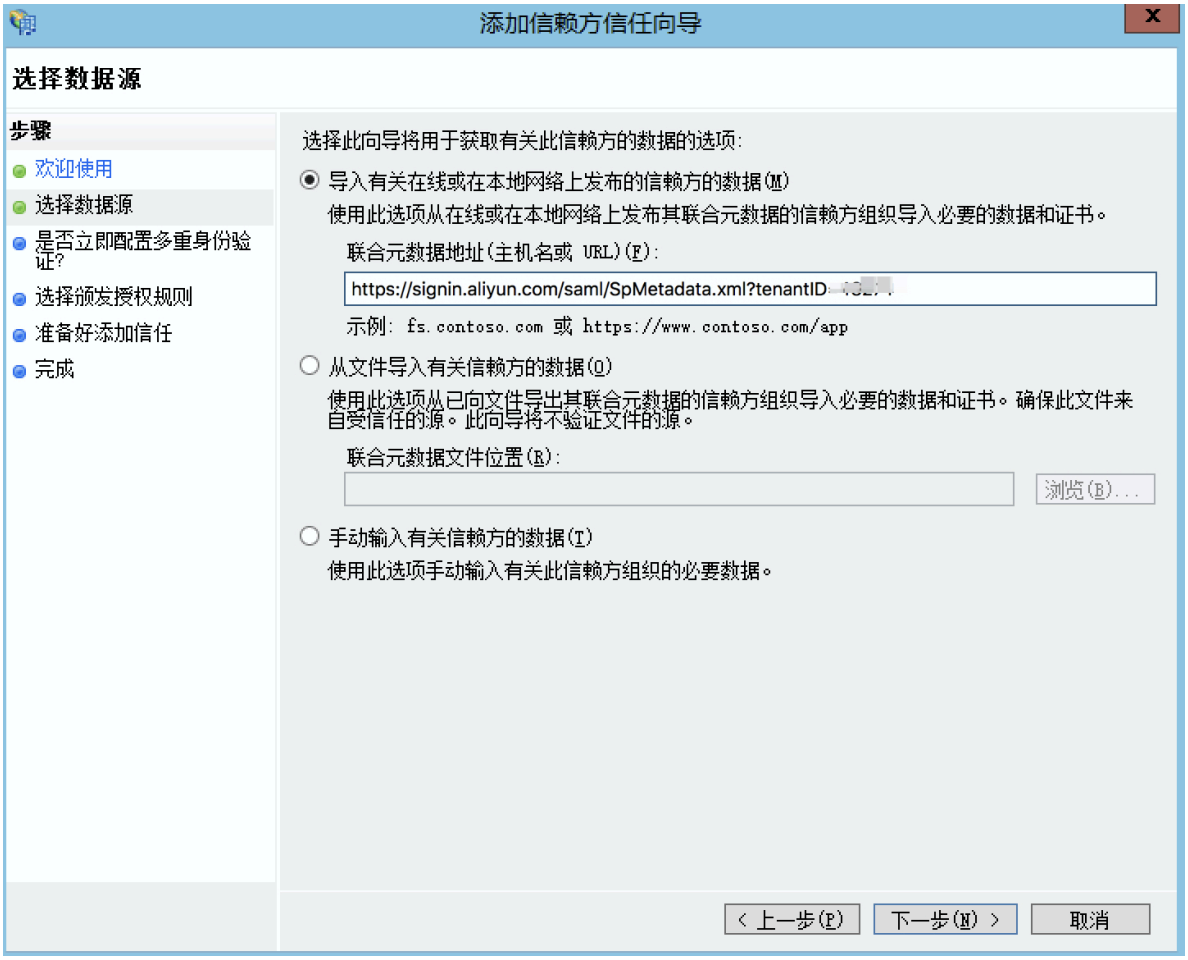


2. 在 AD FS 管理工具中添加信赖方信任。



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。

为阿里云 SP 配置 SAML 断言属性

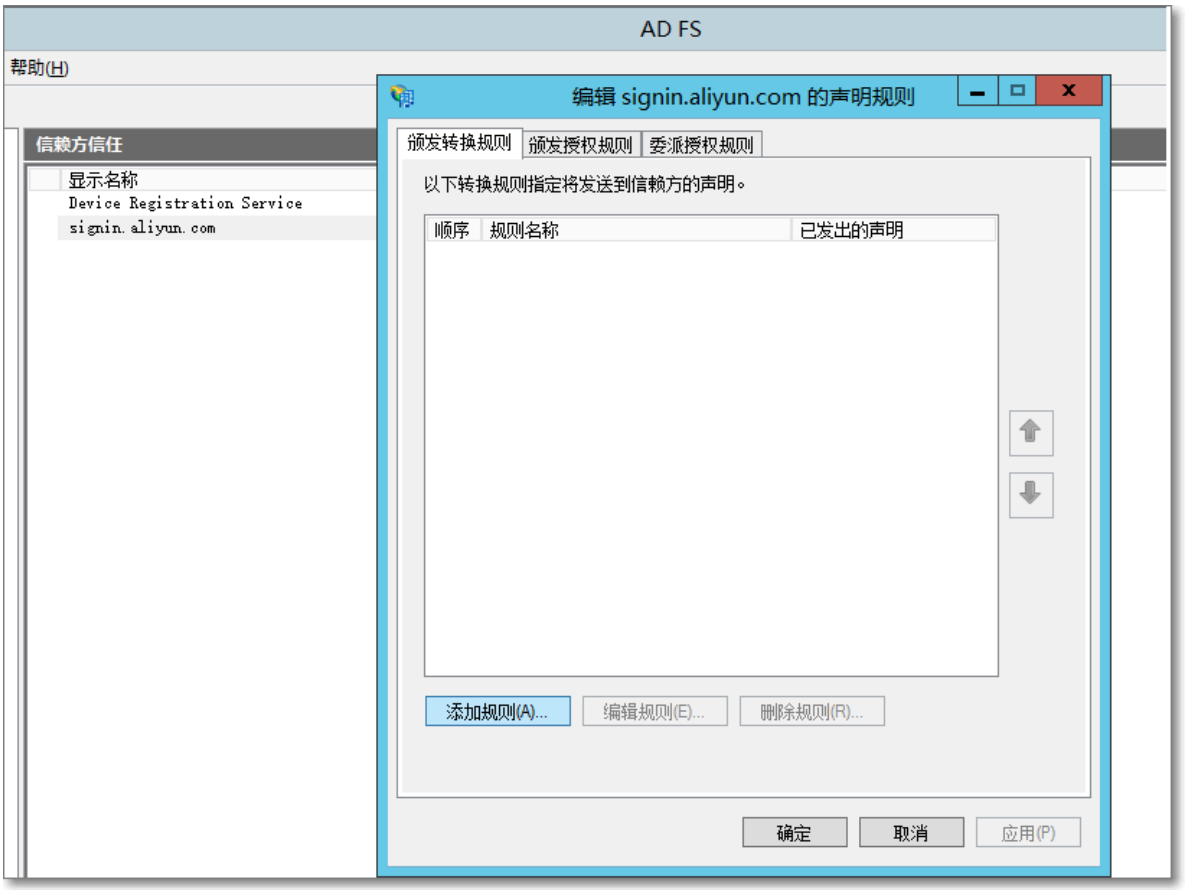
为了让阿里云能使用 SAML 响应定位到正确的 RAM 用户，SAML 断言中的 `NameID` 字段取值应为 RAM 用户的 UPN。

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:

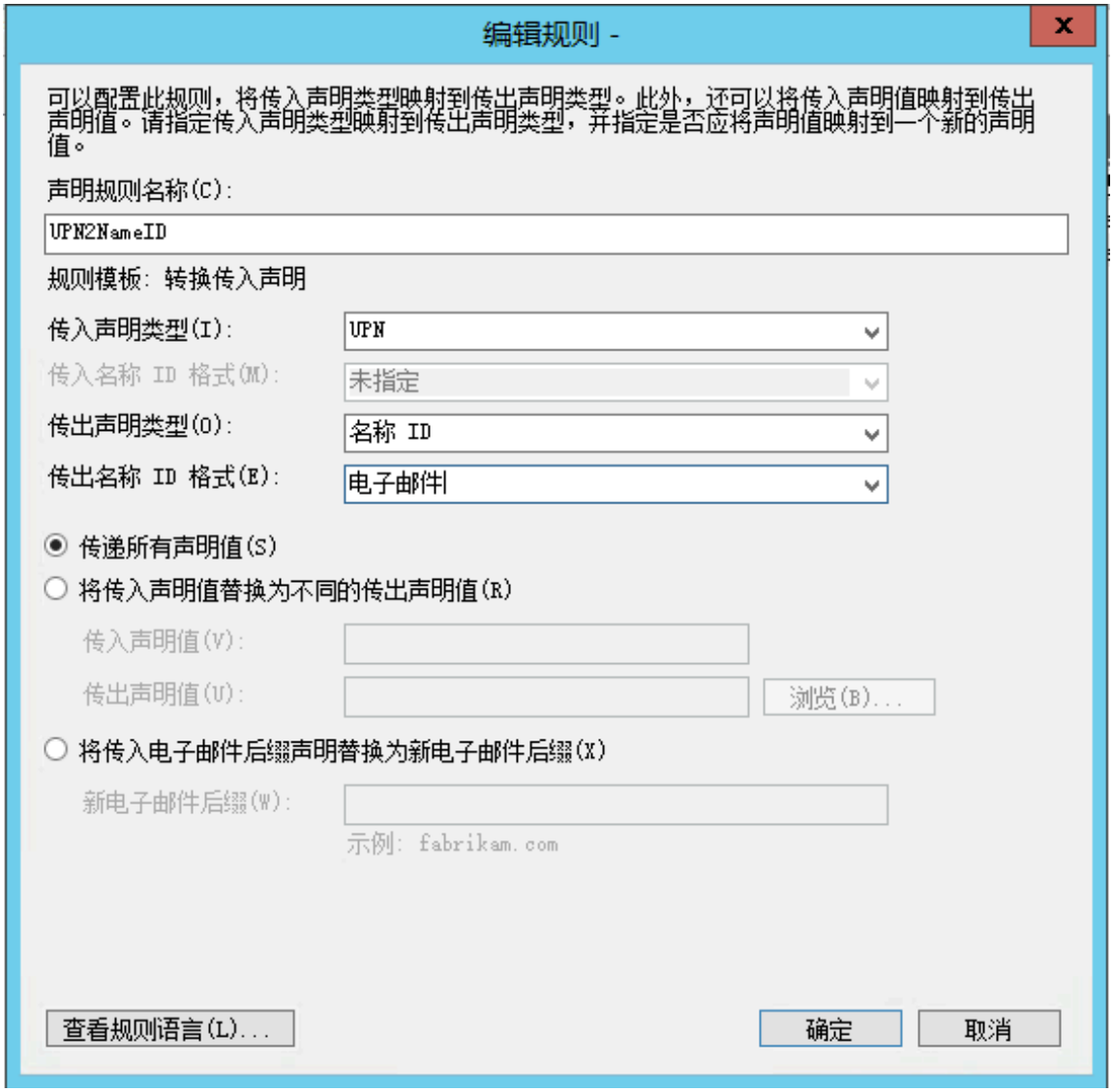
由于示例中的云账号里的 UPN 域名为secloud.onaliyun.com，而 AD 中的 UPN 域名为secloud.club，如果直接将 AD 中的 UPN 映射为NameID，阿里云将无法匹配到正确的 RAM 用户。

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：

a. 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，请参考：#unique_16。

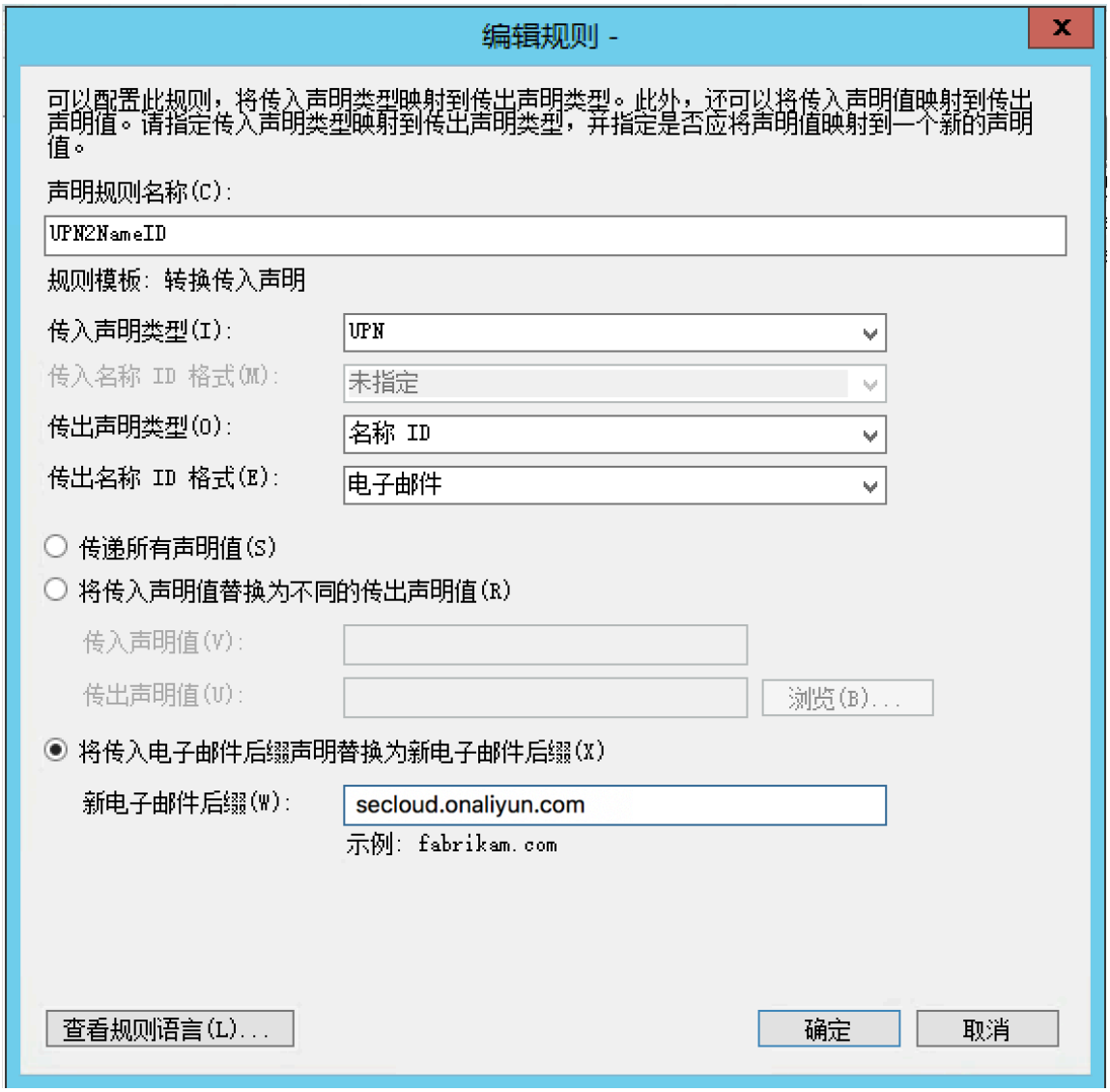
完成设置后，在编辑规则窗口，将 UPN 映射为名称 ID（NameID）。



b. 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。

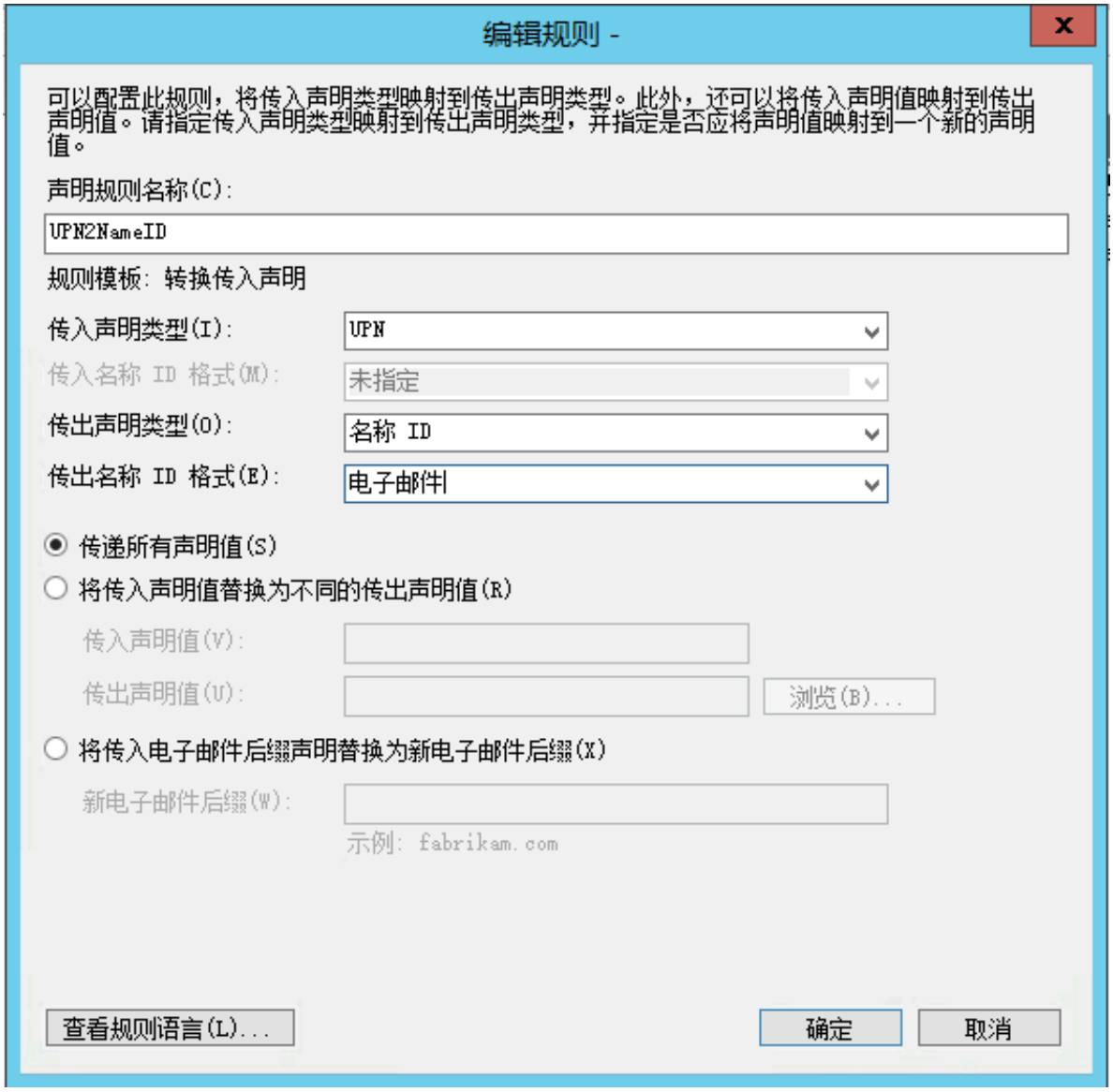
在 AD FS 给阿里云颁发的 SAML 断言中必须将 UPN 的域名后缀从 `secloud.club` 替换为：`secloud.onaliyun.com`。



c. 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，请参考：设置辅助域名。

完成设置后，在编辑规则窗口，将 UPN 映射为名称 ID（`NameID`）。


编辑规则 -
可以配置此规则，将传入声明类型映射到传出声明类型。此外，还可以将传入声明值映射到传出声明值。请指定传入声明类型映射到传出声明类型，并指定是否应将声明值映射到一个新的声明值。
声明规则名称(C):
UPN2NameID
规则模板：转换传入声明
传入声明类型(I):
UPN
传入名称 ID 格式(M):
未指定
传出声明类型(O):
名称 ID
传出名称 ID 格式(E):
电子邮件
传递所有声明值(S)
将传入声明值替换为不同的传出声明值(R)
传入声明值(V):
传出声明值(U):
浏览(B)...
将传入电子邮件后缀声明替换为新电子邮件后缀(X)
新电子邮件后缀(W):
示例: fabrikam.com
查看规则语言(L)...
确定
取消

4 角色SSO

4.1 进行角色SSO

本文为您介绍角色SSO的背景、基本流程以及配置步骤。

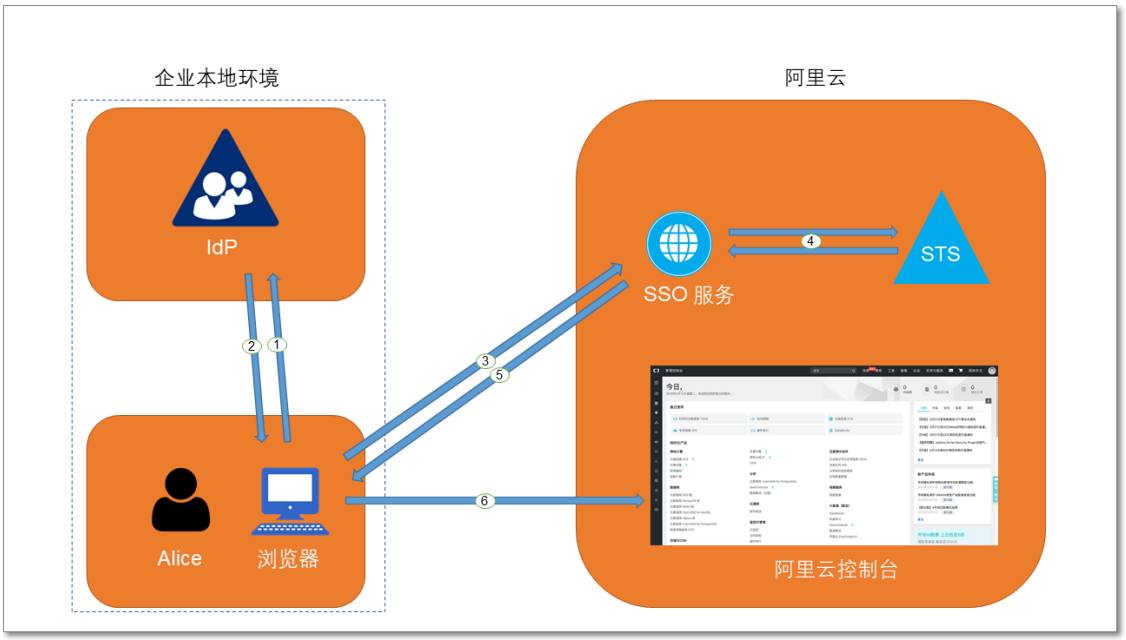
背景信息

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 角色来登录阿里云。

基本流程

通过角色SSO，企业员工既可以通过控制台也可以使用程序访问阿里云。

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可以通过如图所示的方法登录到阿里云。

1. 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`。

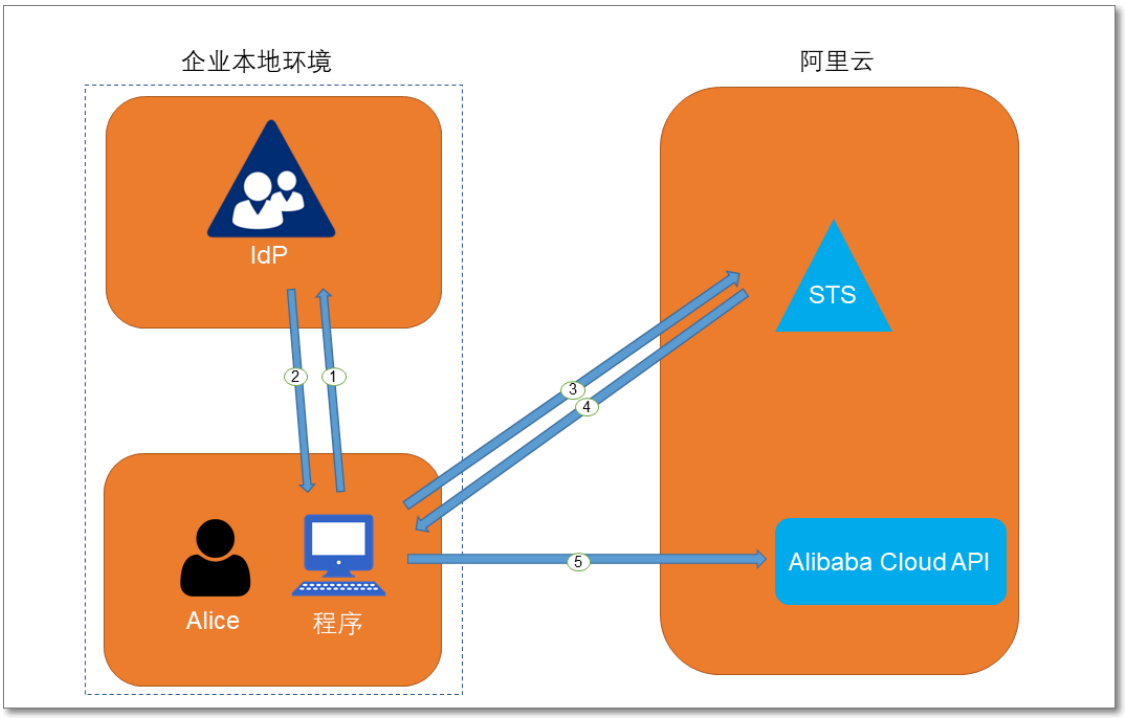
   > **说明:**
   > 有些IdP会要求用户先登录，再选择代表阿里云的SSO应用。

2. IdP生成一个SAML响应并返回给浏览器。
3. 浏览器重定向到SSO服务页面，并转发SAML响应给SSO服务。
4. 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。

5. SSO服务将URL返回给浏览器。
6. 浏览器重定向到该URL，以指定角色身份登录到阿里云控制台。

使用程序访问阿里云



企业员工Alice可以通过编写程序来访问阿里云，基本流程如图所示：

1. Alice使用程序向企业IdP发起登录请求。
2. 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。
3. 程序调用阿里云STS服务提供的API #unique_22，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。
4. STS服务将校验SAML断言并返回临时安全凭证给程序。
5. 程序可以开始使用临时安全凭证来调用阿里云API。

角色SSO的配置步骤

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。

   详情请参见阿里云角色SSO的SAML配置。

2. 企业需要使用程序或登录RAM控制台创建用于SSO的角色，并授予相关权限。

   详情请参见#unique_24。

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。

   详情请参见进行角色SSO时企业IdP的SAML配置。

后续步骤

由于不同IdP的系统差异，关于SAML SP配置和断言属性配置的操作流程都有些差异。我们会提供一个以AD FS与阿里云进行角色SSO的示例，用于帮助理解企业IdP与阿里云的端到端配置流程。

详情请参见#unique_26。

4.2 身份提供商

4.2.1 创建身份提供商

在使用角色SSO时，需要创建身份提供商。

操作步骤

1. 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页签下，单击新建身份提供商。
4. 输入提供商名称和备注。
5. 在元数据文档处，单击上传文件。

   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、用于验证签名的公钥及断言格式等信息。

6. 单击确定。

4.2.2 查看身份提供商基本信息

本文为您介绍如何查看身份提供商基本信息，包括身份提供商名称、ARN和备注等信息。

操作步骤

1. 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页签下，单击目标身份提供商名称。
4. 在身份提供商信息页面下，可以查看身份提供商基本信息。

4.2.3 修改身份提供商基本信息

本文为您介绍如何修改身份提供商基本信息，包括备注和元数据文档。

操作步骤

1. 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页签下，单击目标身份提供商名称。
4. 在身份提供商信息页面下，单击编辑。

   说明:
   身份提供商名称不允许修改。修改身份提供商名称会导致与其受信实体信息不一致，无法正常进行单点登录（SSO）。
5. 修改完成后，单击确认。

4.2.4 删除身份提供商

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

操作步骤

1. 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页签下，找到目标身份提供商，单击删除。
4. 单击确认。

4.3 阿里云角色SSO的SAML配置

本文介绍如何通过基于SAML 2.0的角色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通过角色SSO登录阿里云。

操作步骤

1. 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页签下，单击新建身份提供商。
4. 输入提供商名称和备注。
5. 在元数据文档处，单击上传文件。

   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、用于验证签名的公钥及断言格式等信息。
6. 单击确定。

后续步骤

创建身份提供商后，必须创建一个或多个RAM角色，该RAM角色的可信实体类型为身份提供商，从而建立企业IdP与阿里云的关联。

单击前往新建RAM角色可直接跳转到创建RAM角色的界面。关于RAM角色的创建，请参见#unique_24。

4.4 进行角色SSO时企业IdP的SAML配置

本文主要介绍企业在使用角色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. 企业IdP的SAML SP配置需要使用阿里云的SAML服务提供商元数据URL：`https://signin.aliyun.com/saml-role/sp-metadata.xml`。
   a) 云账号登录 RAM控制台。
   b) 在左侧导航栏，单击SSO管理。
   c) 在角色SSO 页签下查看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：

   - 直接使用上述阿里云的元数据URL进行配置。
   - 如果您的IdP不支持URL配置，您可以根据上述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`
     - `ACS URL: https://signin.aliyun.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：

       您只能填写`*.console.aliyun.com`域名下的URL作为`RelayState`的值。

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。

阿里云要求企业IdP生成的SAML断言里包含一些必要的信息以确定企业用户的登录身份，因此企业IdP必须进行属性配置来匹配RAM角色，从而实现企业用户与阿里云的SSO。

具体需要配置的SAML断言属性请参见c72e1357747c8019b1a5aa7a4f4e46c376dfa9df.dita。

4.5 支持角色SSO的SAML断言

本文介绍在进行角色SSO时，您的IdP颁发的SAML断言必须具备的属性元素。

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 2.0协议的通用元素

- `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。

- 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协议的定义来给出NameID的值，但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必须有如下两个属性：
    - 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.aliyun.com/saml-role/sso。

  如下是一个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.aliyun.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。

  如下是一个Conditions元素的示例：

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

阿里云要求的自定义属性

在SAML断言的AttributeStatement元素中，必须包含如下阿里云要求的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，中间用英文逗号（,）隔开。这两个ARN您可以在控制台获取：

  - 角色ARN：在RAM角色管理页面，单击RAM角色名称后，基本信息页面可以查看对应的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后，身份提供商信息页面可以查看对应的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。

  如下是一个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32个字符，只能是英文字母、数字和以下特殊字符：-_.@=,+。

  如下是一个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。在通过控制台登录的情况下，其包含的AttributeValue元素取值将会被作为用户会话的有效时长。在通过程序登录的情况下，其包含的AttributeValue元素取值无效。

  其AttributeValue元素取值要求：整数，单位为秒，最小900秒（15分钟），最大3600秒（1小时）。若此元素不存在，则取默认值3600秒。

  如下是一个SessionDuration Attribute元素示例：

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

4.6 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。

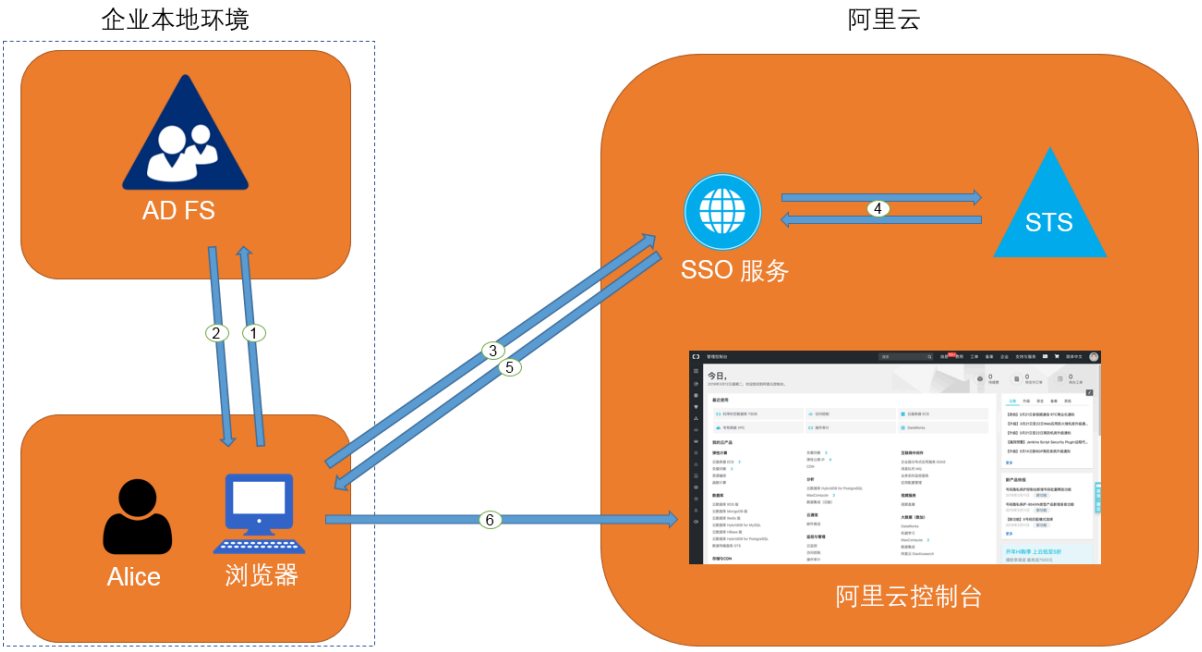
场景

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，企业想要实现从 AD FS 到 Account1 和 Account2 的 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。

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。详情请参见#unique_34。

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。

配置步骤

为了实现上述登录过程，管理员需要在阿里云和 AD FS 上进行以下配置：

- 在阿里云中将 AD FS 配置为可信 SAML IdP。
  1. 在阿里云 RAM 控制台创建一个名为`ADFS`的身份提供商，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。

     详情请参见#unique_35。
  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，并对两个角色分别赋予`AdministratorAccess`和`ReadOnlyAccess`权限。详情请参见#unique_36。
  3. 使用同样的方法在 Account2 中创建同样的身份提供商和角色。

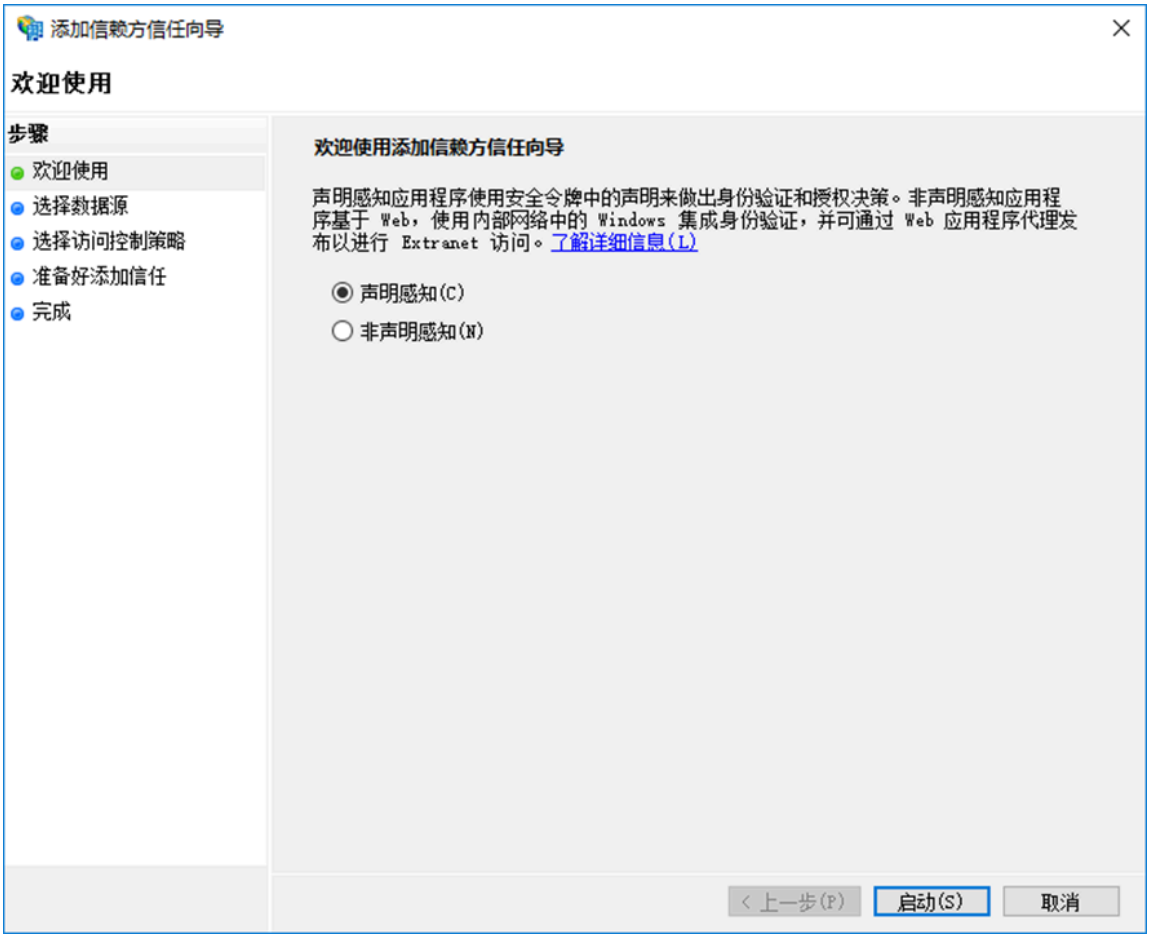
     > **说明:**

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。

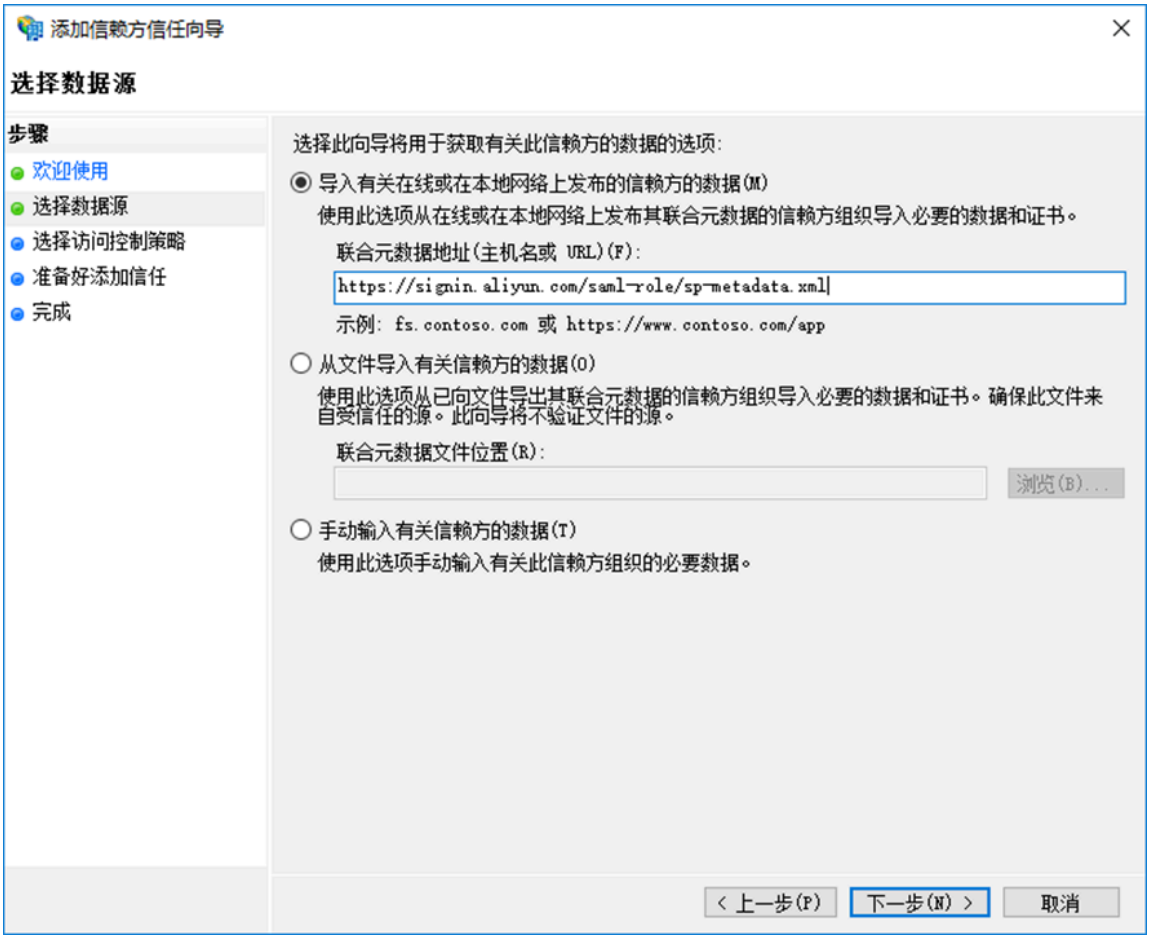
- 在 AD FS 中将阿里云配置为可信 SAML SP。

  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.aliyun.com/saml-role/sp-metadata.xml`。



4. 按照向导完成配置。

- 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`，`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：

    1. 为信赖方编辑声明规则。
    2. 添加颁发转换规则。

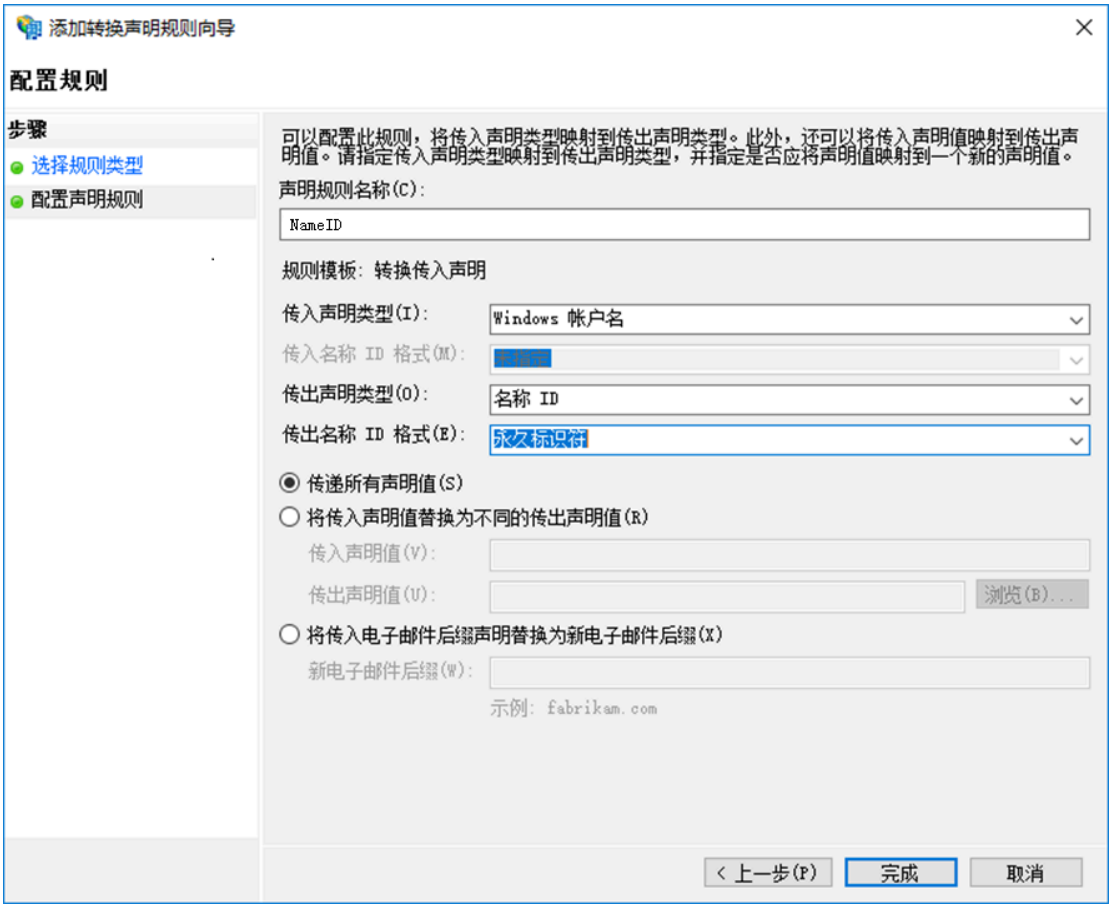
    > **说明:**

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 Windows 账户名颁发为`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. 使用如下配置规则，并点击完成。

- 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，如下：

```
<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：

  1. 单击添加转换声明规则。
  2. 从声明规则模板中选择以声明方式发送 LDAP 特性。

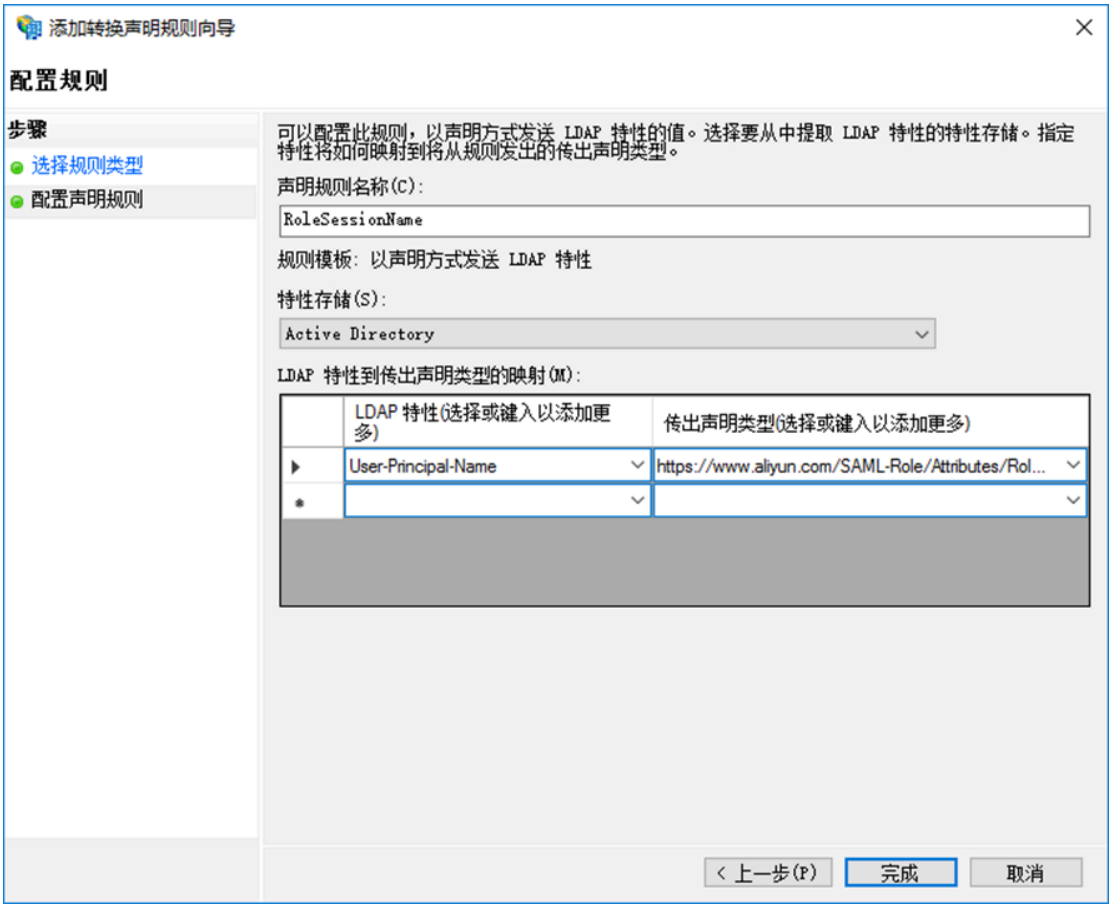
  3. 使用如下配置规则，并点击完成。

     ■ 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，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，如下：

```
<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：

1. **单击添加转换声明规则。**
2. **从声明规则模板中选择使用自定义规则发送声明，点击下一步。**

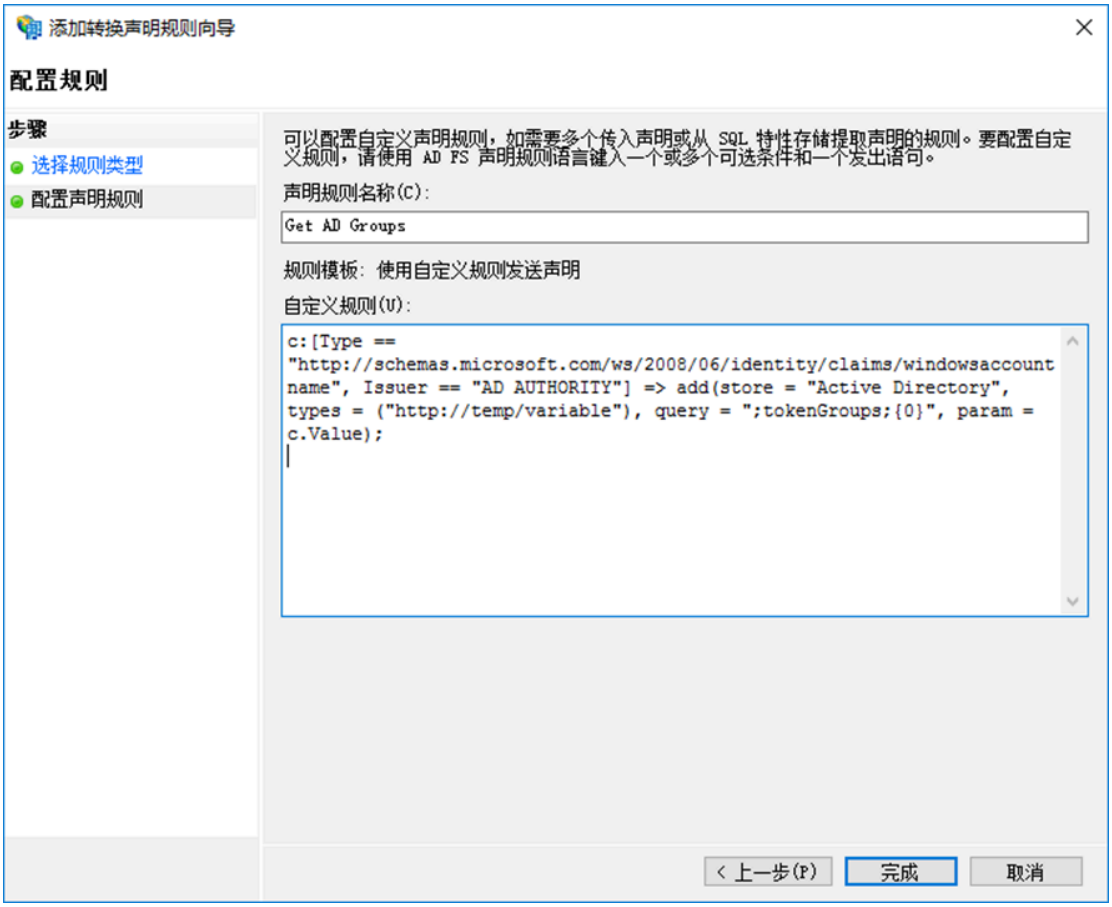
3. **使用如下配置规则，并点击完成。**

   ■ **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/
windowsaccount
name", Issuer == "AD AUTHORITY"] => add(store = "Active
Directory",
types = ("http://temp/variable"), query = ";tokenGroups;{0
}", param =
```

```
c.Value);
```



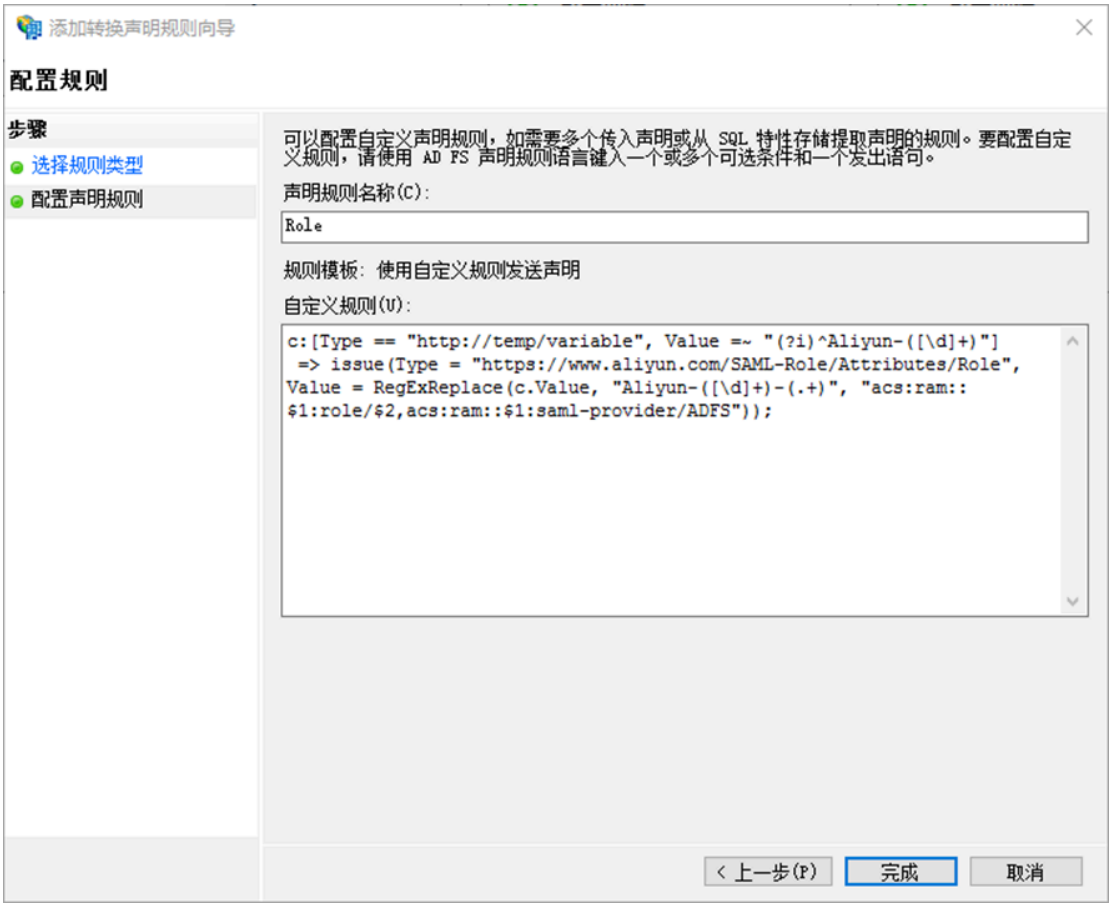
说明:

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。

4. **单击添加转换声明规则。**
5. **重复以上步骤，并点击完成。**
   - **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：

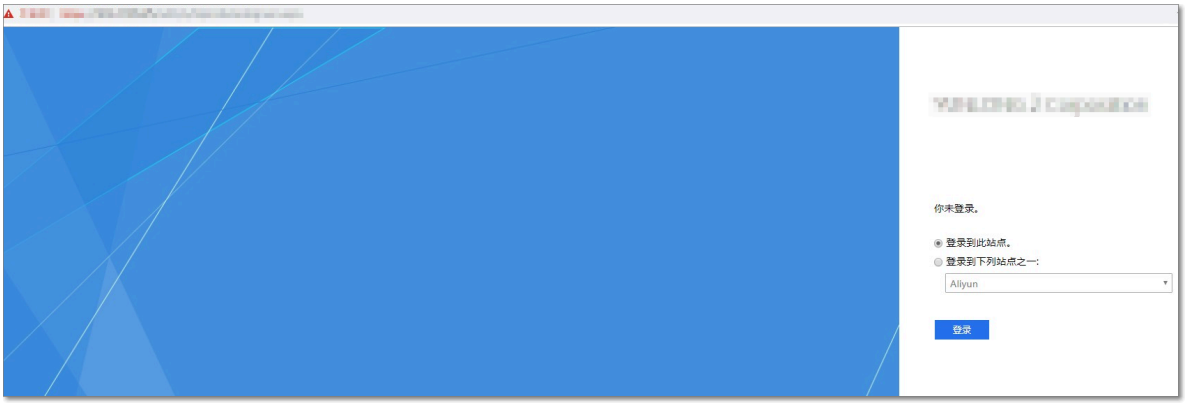
```
<Attribute Name="https://www.aliyun.com/SAML-Role/Attributes/Role
">
    <AttributeValue>acs:ram::<account-id>:role/ADFS-Admin,acs:ram
::<account-id>:saml-provider/ADFS</AttributeValue>
</Attribute>
```

配置验证

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。**

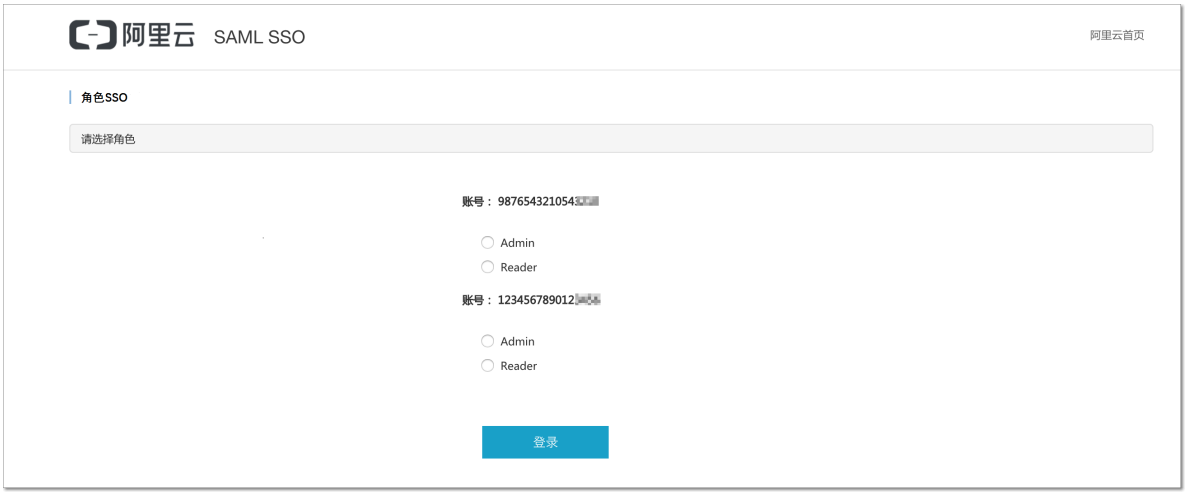
说明:

<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。

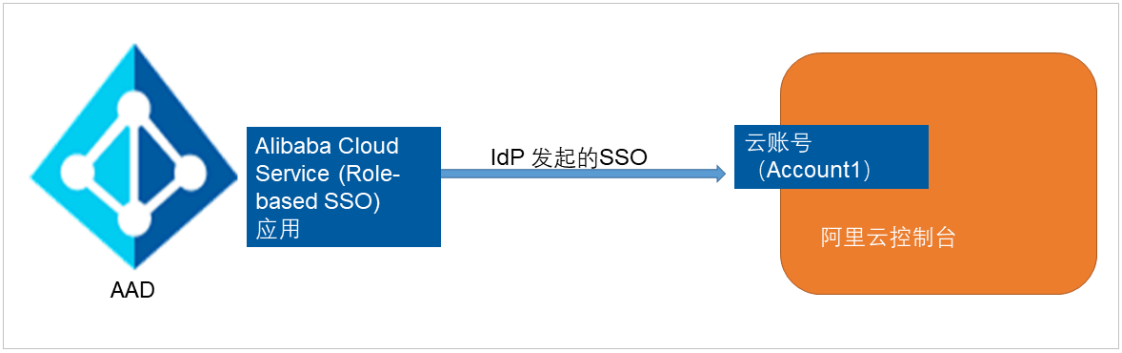


4.7 使用Azure AD进行角色SSO的示例

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）和一个企业员工用户（u2）。企业可以使用AAD进行员工管理，并通过AAD配置包括阿里云在内的企业应用。配置完成后，您可以更好的管理企业员工，企业员工也可以实现从AAD到阿里云的角色SSO。

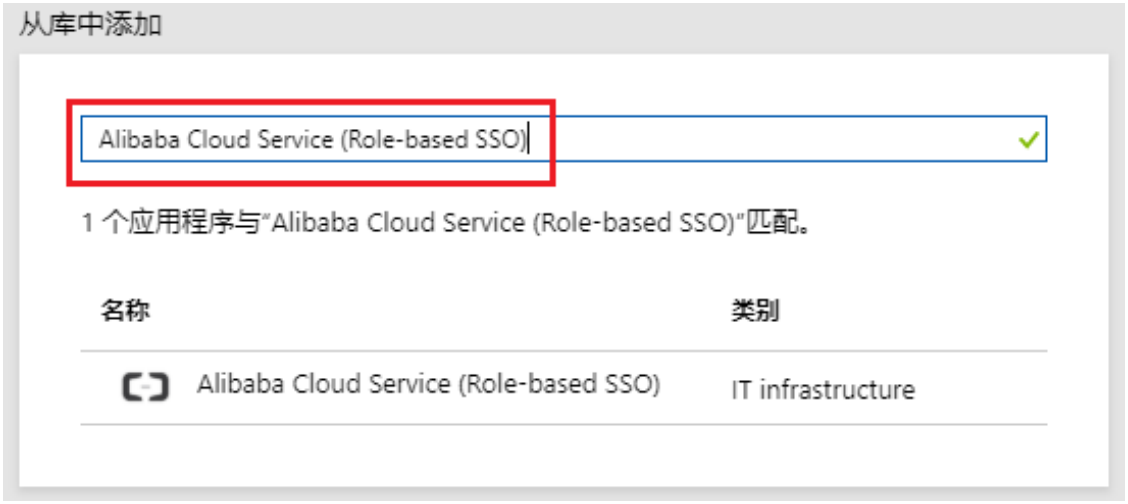


在AAD库中添加应用程序

1. 管理员登录Azure门户。
2. 在左侧导航栏，单击Azure Active Directory > 企业应用程序 > 所有应用程序。

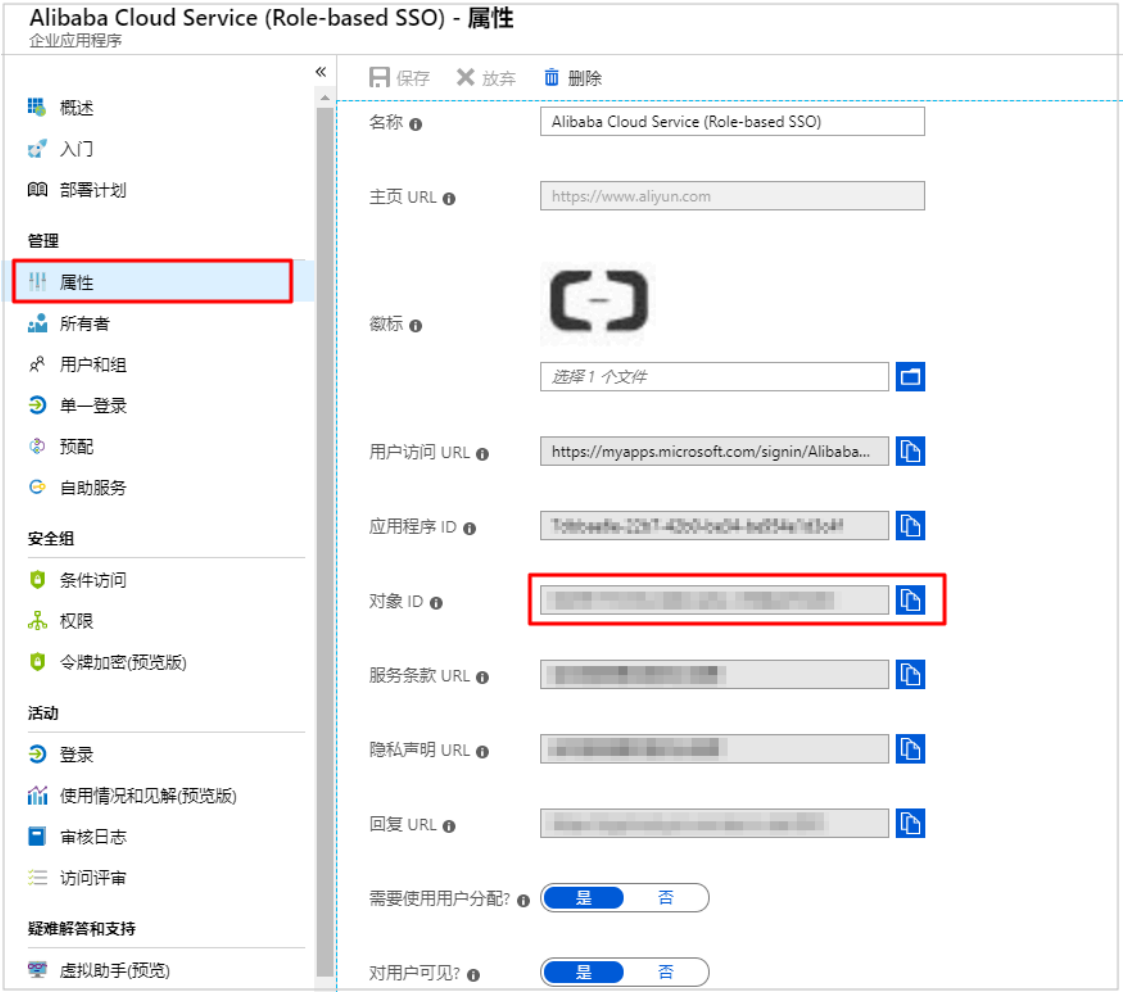
3. 单击新建应用程序。

4. 在添加应用程序页面下的从库中添加搜索区域，输入Alibaba Cloud Service（Role-based SSO）并单击选择。



5. 单击添加。

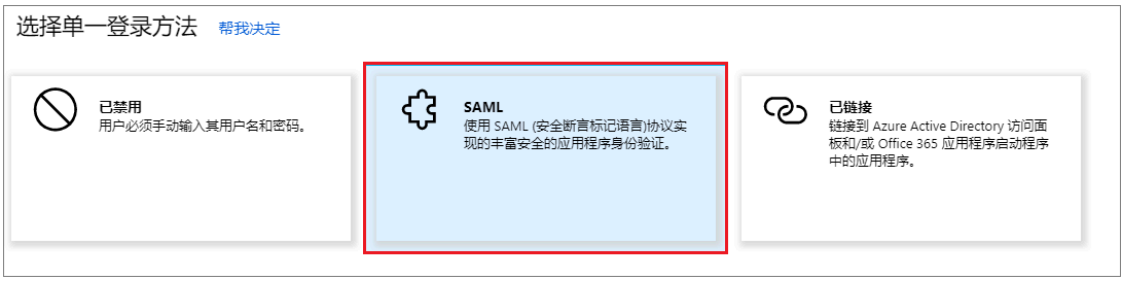
6. 在Alibaba Cloud Service（Role-based SSO）页面下，单击左侧导航栏下的属性，复制并保存对象ID。



配置AAD SSO

1. 管理员登录Azure门户。
2. 在左侧导航栏，单击Azure Active Directory > 企业应用程序 > 所有应用程序。
3. 在名称列表下，单击Alibaba Cloud Service（Role-based SSO）。
4. 在左侧导航栏，选择单一登录。

5. 在选择单一登录方法页面下，单击SAML。



6. 在设置SAML单一登录页面进行配置。

a) 在页面左上角，单击上传元数据文件，选择文件后，单击添加。

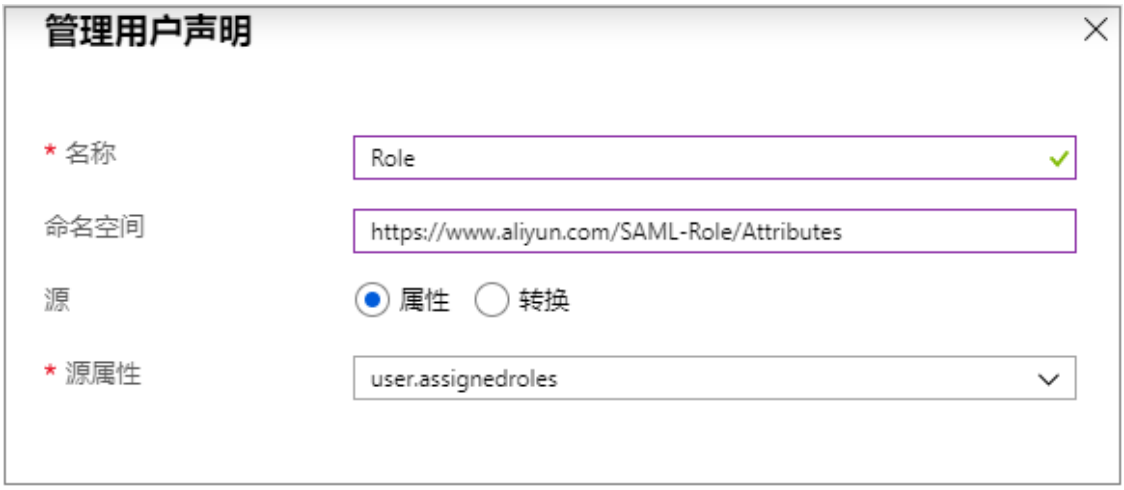
说明:

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

b) 在用户属性和声明区域，单击编辑图标。

c) 单击添加新的声明，设置以下配置后，单击保存。

- 在名称区域下，输入`Role`。
- 在命名空间区域下，输入`https://www.aliyun.com/SAML-Role/Attributes`。
- 在源区域下，选择属性。
- 在源属性区域下，从下拉列表中选择`user.assignedroles`。

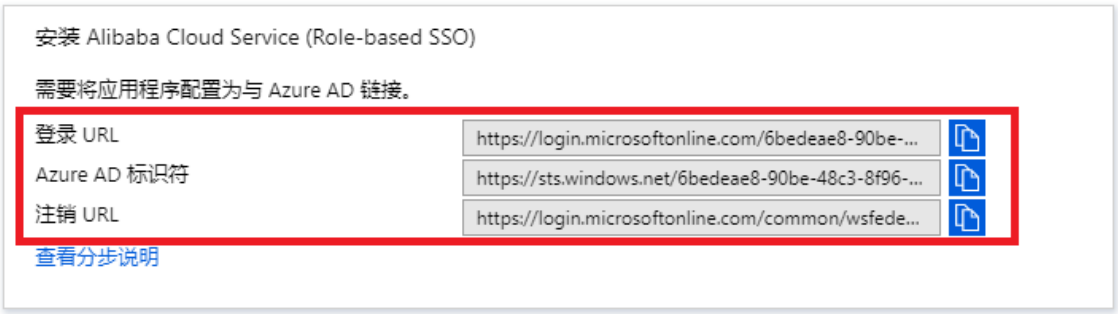


d) 重复上述步骤，添加一个新的声明。

- 在名称区域下，输入`RoleSessionName`。
- 在命名空间区域下，输入`https://www.aliyun.com/SAML-Role/Attributes`。
- 在源区域下，选择属性。
- 在源属性区域下，从下拉列表中选择`user.userprincipalname`。

e) 在SAML签名证书区域下的联合元数据XML，单击下载。

f) 在安装Alibaba Cloud Service（Role-based SSO）区域下，复制登录URL、Azure AD标识符和注销URL。



在阿里云配置角色SSO

1. 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页签下，单击新建身份提供商。
4. 输入提供商名称AAD和备注。
5. 在元数据文档处，单击上传文件。

> **说明:**
> 上传上述步骤中在SAML 签名证书区域下载的联合元数据XML。

6. 单击确定。
7. 创建身份提供商后，单击前往新建RAM角色。
8. 输入角色名称AADrole和备注。
9. 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#unique_38。

- 当身份提供商和对应的RAM角色后，请保存好对应的ARN。关于如何查看ARN，请参见#unique_39。

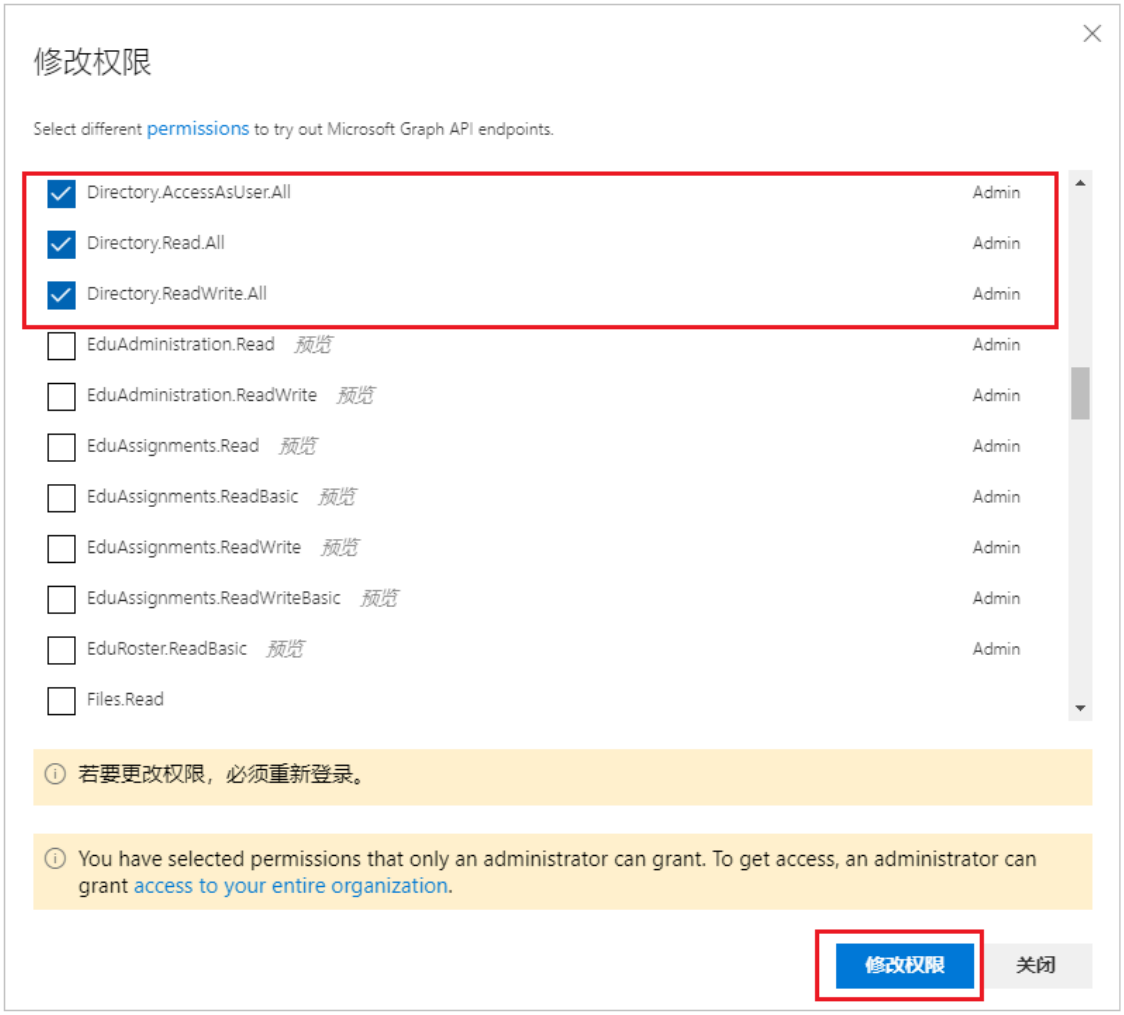
将阿里云RAM角色与AAD用户进行关联

1. **在AAD中创建角色。**

   a) **用户（u2）登录AAD Graph浏览器。**

   b) **单击修改权限。**

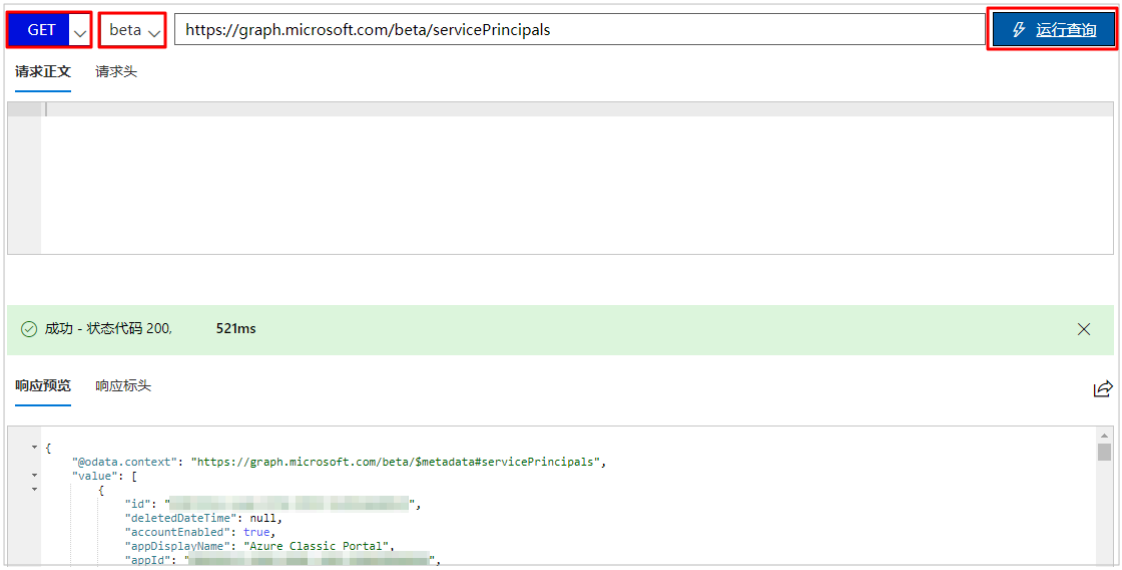
   c) **从下拉列表中选择以下权限并单击修改权限。**



说明:

修改权限后，系统会重定向到Graph浏览器。

d) **在Graph浏览器页面，第一个下拉列表中选择GET，第二个下拉列表中选择beta。在搜索框中输入**`https://graph.microsoft.com/beta/servicePrincipals`**并单击运行查询。**



说明:

如果您有多个目录，您可以在查询区域输入`https://graph.microsoft.com/beta/contoso.com/servicePrincipals`**。**

e) **在响应预览页签下，从**`Service Principal`**中提取出**`appRoles`**属性并保存。**

```
"appRoles": [
                {
                    "allowedMemberTypes": [
                        "User"
                    ],
                    "description": "msiam_access",
                    "displayName": "msiam_access",
                    "id": "7dfd756e-8c27-4472-b2b7-38c17fc5****",
                    "isEnabled": true,
                    "origin": "Application",
                    "value": null
                }
            ],
```

说明:

您可以在查询字段中输入https://graph.microsoft.com/beta/servicePrincipals/<objectID>来定位appRoles属性，其中objectID是您在AAD属性页面保存的。

f）返回Graph浏览器，将第一个下拉列表改为PATCH，第二个下拉列表中选择beta。在搜索框中输入https://graph.microsoft.com/beta/servicePrincipals/<objectID>，将以下内容复制到请求正文中并选择运行查询。

```
{
  "appRoles": [
    {
      "allowedMemberTypes":[
        "User"
      ],
      "description": "msiam_access",
      "displayName": "msiam_access",
      "id": "41be2db8-48d9-4277-8e86-f6d22d35****",//appRoles的ID
      "isEnabled": true,
      "origin": "Application",
      "value": null
    },
    { "allowedMemberTypes": [
        "User"
    ],
    "description": "Admin,AzureADProd",
    "displayName": "Admin,AzureADProd",
    "id": "68adae10-8b6b-47e6-9142-6476078c****",//ID生成器（例如:
GUID生成器）实时生成的ID
    "isEnabled": true,
    "origin": "ServicePrincipal",
    "value": "acs:ram::187125022722****:role/aadrole,acs:ram::
187125022722****:saml-provider/AAD"//身份提供商和RAM角色的ARN
    }
  ]
}
```

说明:

您可以根据需要创建多个RAM角色，AAD将在SAML中将这些角色作为声明值进行传送，但是您只能在msiam_access后添加新的角色。

2. 将RAM角色添加到用户（u2）中。

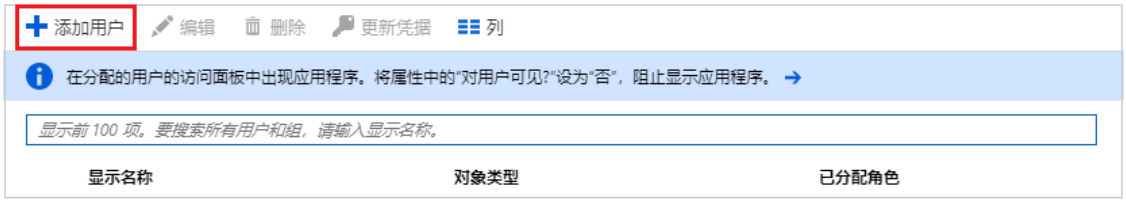
a) 管理员登录Azure门户。

b) 在左侧导航栏，单击Azure Active Directory > 企业应用程序 > 所有应用程序。

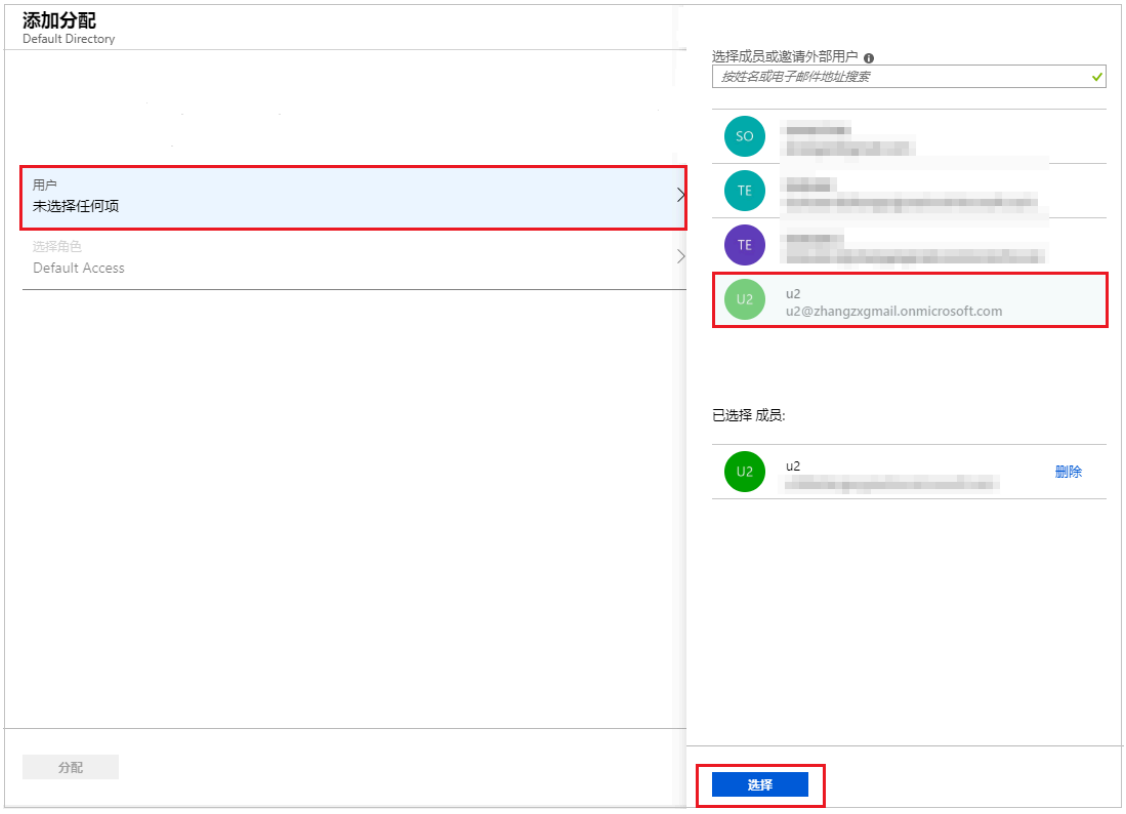
c) 在名称列表下，单击Alibaba Cloud Service（Role-based SSO）。

d) 在左侧导航栏，单击用户和组。

e) 单击左上角的添加用户。

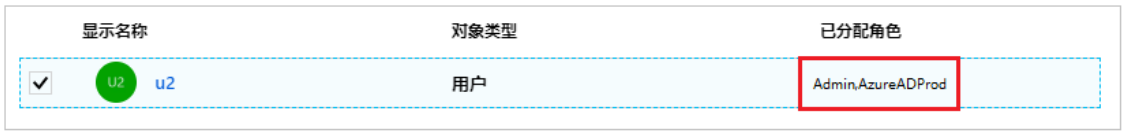


f) 单击用户，从用户列表中选择用户（u2），单击选择。



g) 单击分配。

h) 查看分配的角色。

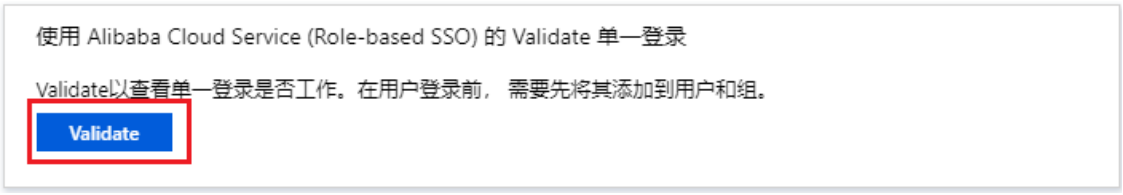


说明:

如果您分配了用户（u2），创建好的RAM角色会自动附加给用户。如果您创建了多个角色，您需要根据需要合理分配角色。如果您需要完成AAD与多个阿里云账号的角色SSO，请重复上述配置步骤。

测试角色SSO

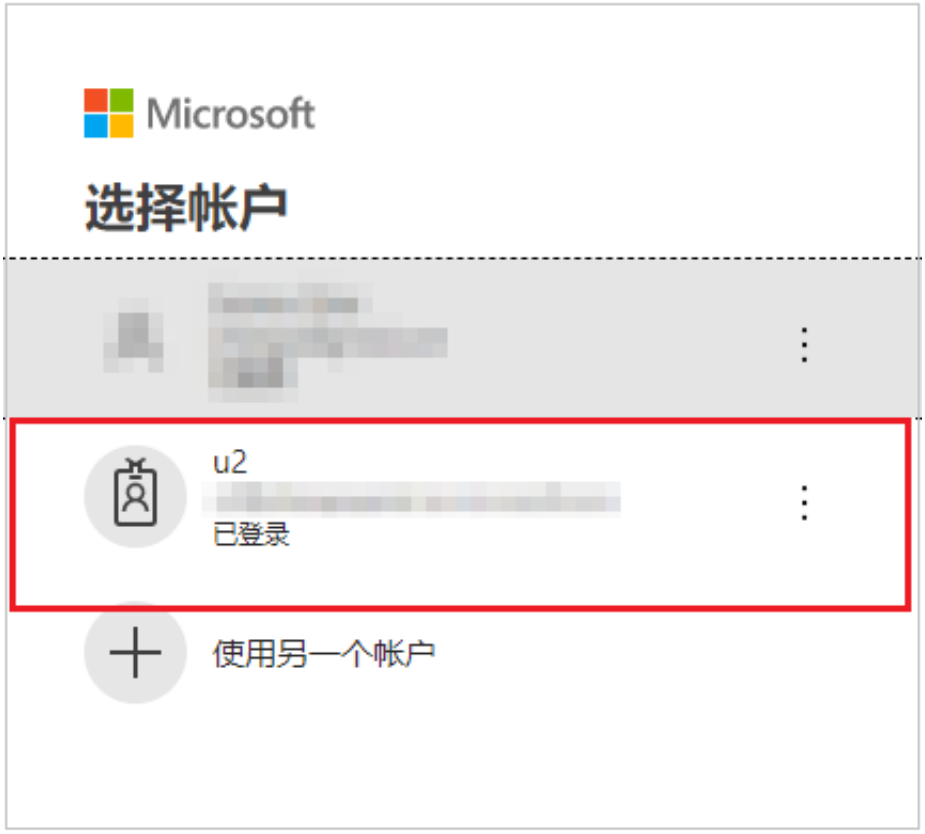
1. 管理员登录Azure门户。
2. 在左侧导航栏，单击Azure Active Directory > 企业应用程序 > 所有应用程序。
3. 在名称列表下，单击Alibaba Cloud Service（Role-based SSO）。
4. 在左侧导航栏，选择单一登录。
5. 在使用Alibaba Cloud Service（Role-based SSO）的Validate单一登录区域下，单击Validate。



说明：
用户（u2）登录前，需要先被添加到用户组中。

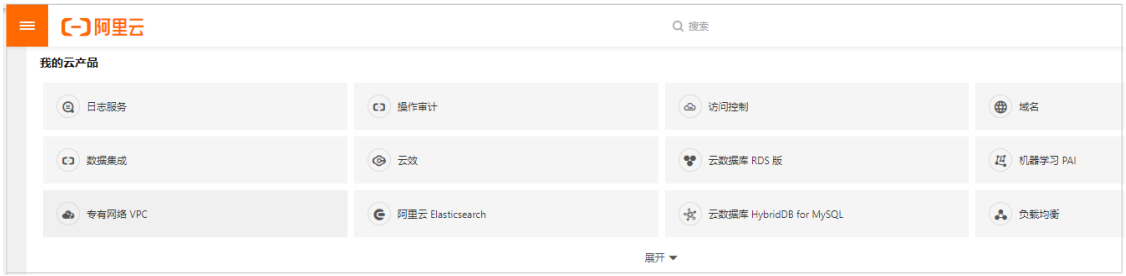
6. 选择作为当前用户登录。

7. 在选择账户页面下，选择用户（u2）。



预期结果

以下界面出现，表示角色SSO成功。



5 最佳实践

5.1 RAM企业上云安全实践

本文为您介绍当企业上云之后，通过RAM进行安全管控，帮助您实现简单管理账号、统一分配权限、集中管控资源，建立安全完善的资源控制体系。

前提条件

进行操作前，请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。

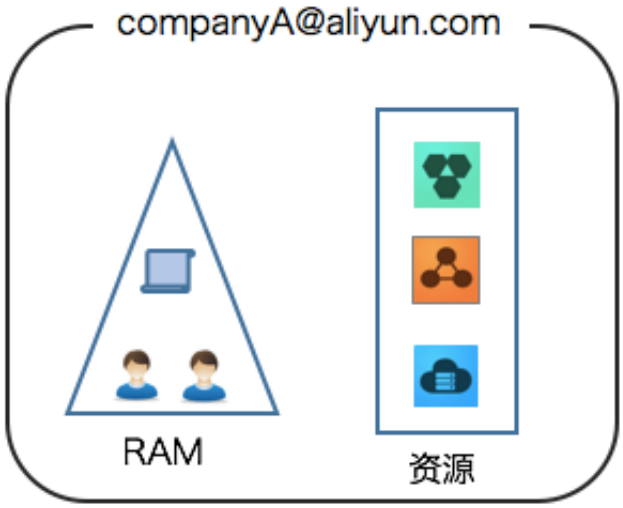
背景信息

某些公司使用RAM初期，对RAM的优势不够了解，也对云资源的安全管理要求不高。但是当初创企业成长为大型公司或大型企业客户迁移上云，组织结构更加复杂，对云资源的安全管理需求也更加强烈，需要建立安全完善的资源控制体系。

- 存在多用户协同操作，RAM用户分工不同，各司其职。
- 云账号不想与其他RAM用户共享云账号密钥，密钥泄露风险较大。
- RAM用户对资源的访问方式多种多样，资源泄露风险高。
- 某些RAM用户离开组织时，需要收回其对资源的访问权限。

解决方案

使用RAM，您可以创建、管理RAM用户，并可以控制这些RAM用户对资源的操作权限。当您的企业存在多用户协同操作资源时，使用RAM可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，管理更加方便，权限更加明确，信息更加安全。



安全管理实施方案

- 创建独立的RAM用户

  企业只需使用一个云账号。通过RAM为名下的不同操作员创建独立的RAM用户，进行分权管理，不使用云账号进行日常运维管理。

  详情请参见#unique_13。

- 将控制台用户与API用户分离

  不建议给一个RAM用户同时创建用于控制台操作的登录密码和用于API操作的访问密钥。

  - 对于应用程序账号，只需要通过OpenAPI访问云资源，只需要给它创建访问密钥即可。
  - 对于员工账号，只需要通过控制台操作云资源，只需要设置登录密码即可。

  详情请参见#unique_13。

- 创建用户并进行分组

  当云账号下有多个RAM用户时，可以通过创建用户组对职责相同的RAM用户进行分类并授权。

  详情请参见#unique_42。

- 给不同用户组分配最小权限

  您可以使用系统策略为用户或用户组绑定合理的权限策略，如果您需要更精细粒度的权限策略，也可以选择使用自定义策略。通过为用户或用户组授予最小权限，可以更好的限制用户对资源的操作权限。

  详情请参见#unique_43。

- 为用户登录配置强密码策略

  您可以通过RAM控制台设置密码策略，如密码长度、密码中必须包含元素、密码有效期等。如果允许RAM用户更改登录密码，那么应该要求RAM用户创建强密码并且定期轮换登录密码或访问密钥。

  详情请参见#unique_44。

- 为云账号开启多因素认证

  开启多因素认证（Multi-factor authentication，MFA）可以提高账号的安全性，在用户名和密码之外再增加一层安全保护。启用MFA后，用户登录阿里云时，系统将要求输入两层安全要素：

  1. 第一安全要素：用户名和密码
  2. 第二安全要素：多因素认证设备生成的验证码

  详情请参见#unique_45。

- 为用户开启SSO单点登录功能

  开启SSO单点登录后，企业内部账号进行统一的身份认证，实现使用企业本地账号登录阿里云才能访问相应资源。

  详情请参见#unique_46。

- 不要为云账号创建访问密钥

  由于云账号对名下资源有完全控制权限，AccessKey与登录密码具有同样的权力，AccessKey用于程序访问，登录密码用于控制台登录。为了避免因访问密钥泄露带来的信息泄露，不建议您创建云账号访问密钥并使用该密钥进行日常工作。

  您可以通过为RAM用户创建访问密钥，使用RAM用户进行日常工作。

  详情请参见#unique_47。

- 使用策略限制条件来增强安全性

  要求用户必须使用安全信道（例如：SSL）、在指定时间范围或在指定源IP条件下才能操作指定的云资源。

  详情请参见#unique_48。

- 集中控制云资源

  阿里云默认云账号是资源的拥有者，掌握完全控制权。RAM用户对资源只有使用权，没有所有权。这一特性可以方便您对用户创建的实例或数据进行集中控制。

  - 当用户离开组织：只需要将对应的账号移除，即可撤销所有权限。
  - 当用户加入组织：只需创建新的账号，设置登录密码或访问密钥并为 RAM 用户授权。

  详情请参见#unique_49。

- 使用STS给用户授权临时权限

  STS （Security Token Service）是RAM的一个扩展授权服务，使用STS访问令牌可以给用户授予临时权限，您可以根据需要来定义访问令牌的权限和自动过期时间，可以让授权更加可控。

  详情请参见#unique_50。

操作结果

遵循最佳安全实践原则，企业上云之后，综合利用这些保护机制，建立安全完善的资源控制体系，可以更有效的保护账号及资产的安全。

更多信息

企业上云以后通过RAM进行运维划分，根据不同的职责，划分不同的运维人员，方便管理和控制。详情请参见#unique_51。