ALIBABA CLOUD

阿里云

应用身份服务

阿里云应用对接

文档版本：20211130

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.阿里云RAM应用对接

1.1. 使用RAM用户单点登录阿里云控制台

本文为您介绍如何通过RAM用户单点登录到阿里云控制台，实现阿里云控制台的快捷登录，提升员工办公体验。

背景信息

某些企业员工日常办公需访问阿里云控制台，且部分员工拥有多个阿里云主账号，访问不同的主账号需要频繁，耗时长且影响用户体验。

解决方案

IDaaS应用身份服务通过RAM用户单点登录阿里云控制台，如果某个用户有多个阿里云主账号，只需添加多个阿里云控制台应用并用不同名称进行区分，即可实现针对不同阿里云账号控制台的单点登录。

用户也可使用AD账户，或者钉钉扫码等方式登录到阿里云控制台，实现用户认证方式的统一管理和访问。

操作步骤

一、RAM用户准备

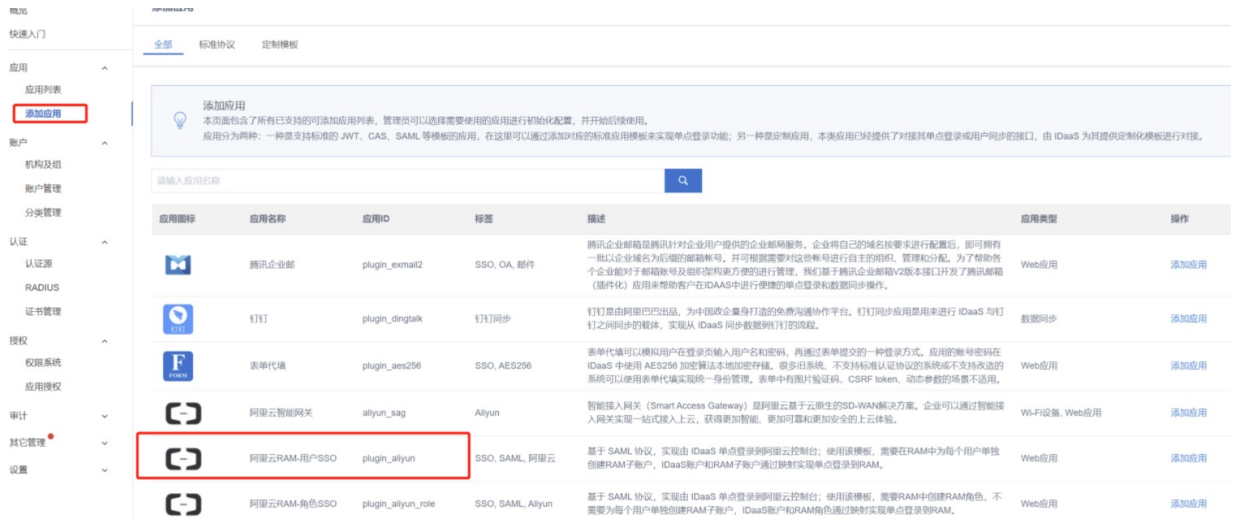
> 说明
> 如果您RAM中已有用户，可以跳过该步骤

1. 使用阿里云账号登录阿里云
2. 搜索访问控制-> 进入RAM控制台。

3. 进入控制台后，点击人员管理中的用户，创建RAM用户

二、IDaaS添加阿里云控制台

1. 应用列表中选择阿里云控制台添加应用



2. 添加SigningKey(证书)

3. 在SigningKey列表界面中右侧点击“选择”进入SAML配置界面。

根据提示填写阿里云个人域名称，IDaaS IdentityId、SP Entity ID和SP ACS URL(SSO Location)等参数并保存，其中红框部分需要替换成阿里云账户ID.

NameIdFomat选择"urm:oasis:names:tc:SAML:2.0:nameid-format:persistent"。

在阿里云控制台点击右上角头像图标，在账号管理-安全设置页面获取阿里云账号ID

也可以通过RAM展示用户位置获取账户ID

4. 保存应用成功，切换到应用列表，查看应用详情

导出SAML元数据文件Metadata.xml

> 说明
> 如果无法导出文件，可能是浏览器拦截了，请修改浏览器设置或者切换浏览器导出。

三、阿里云控制台中配置SSO单点登录

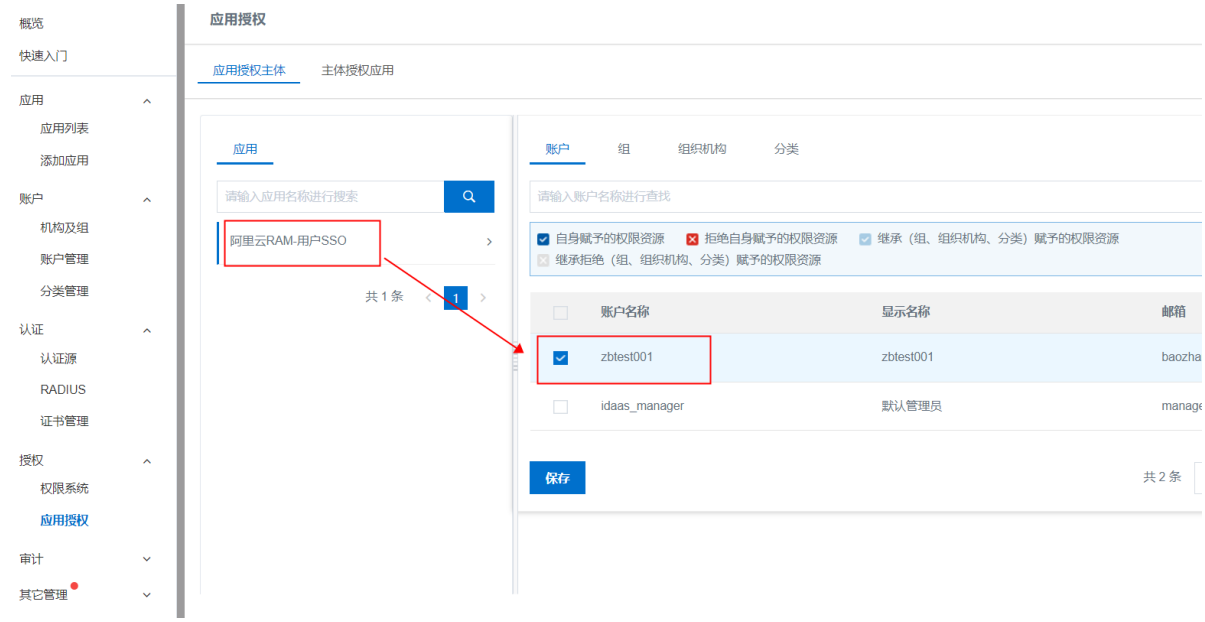
1. 切换到阿里云控制台中上传Metada.xml文件，点击SSO管理-点击“用户SSO”进入页面，开启SSO功能，并上传元文件

四、从IDaaS单点登录到阿里云控制台

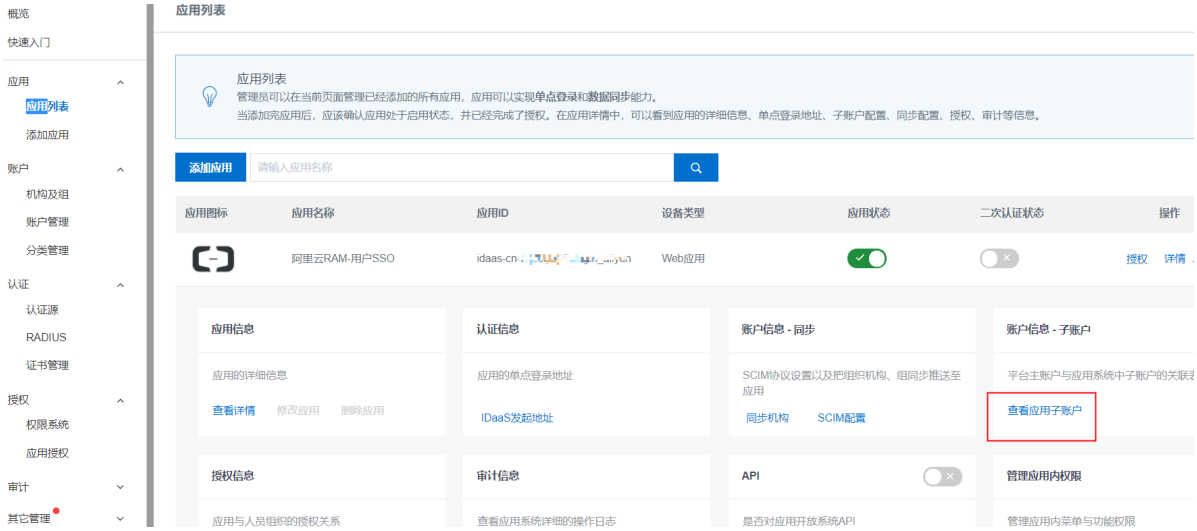
1. 首先确保应用是开启状态

2. 确认在IDaaS中用户是否存在，没有则创建用户

3. 在应用授权模块对应用进行授权



4. 在IDaaS中给应用的主账户绑定子账户，主账户是IDaaS中创建的用户，子账户是阿里云控制台中的RAM用户



主子账户绑定如下图，zetest001是在IDaaS中创建的账户，作为主账户；RAM-user是RAM中的账户，作为子账户，子账户只需要输入RAM账户名称

5. 在IDaaS实例列表页获取访问普通用户的登录地址，copy下面的链接

6. 输入IDaaS中创建的用户进行登录，登录成功后，点击首页的阿里云控制台图标进行单点登录

若以上步骤全部成功完成，即可实现RAM用户单点登录阿里云控制台。

FAQ

1. 显示下图错误，请确认是否在阿里云RAM控制台上传了metadata文件

2. 显示下图错误，请确认IDaaS IdentityId 和 SP Entity ID的值是否添加正确

3. 如何修改SSO登录后跳转的地址？

修改RelayState的值

4. RAM开启单点登录配置后，原来RAM子账户的登录方式是否还可以继续使用

不可以使用。因为开启RAM的SSO功能后，登录就被IDaaS接管了，访问原来的登录入口会直接跳转到IDaaS登录页面。

1.2. 使用RAM角色单点登录阿里云控制台

本文为您介绍通过RAM角色账号单点登录到阿里云控制台上，实现阿里云控制台的便捷登录，提升员工办公体验。

背景信息

某些企业员工日常办公需访问阿里云控制台，部分员工拥有多个账号，每个账号的权限及角色各不同，传统的登录方式需频繁切换账号，繁琐耗时且影响用户体验。

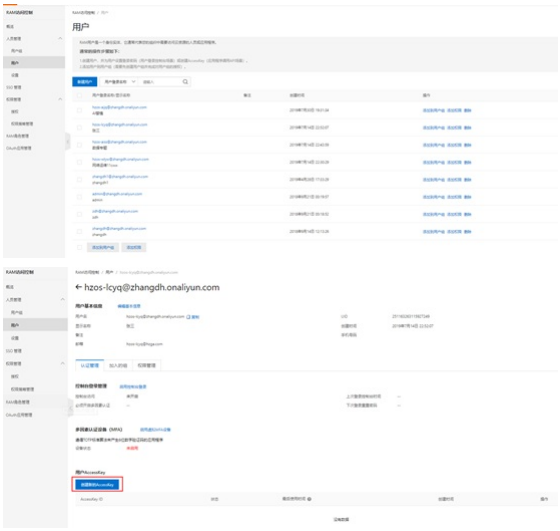
解决方案

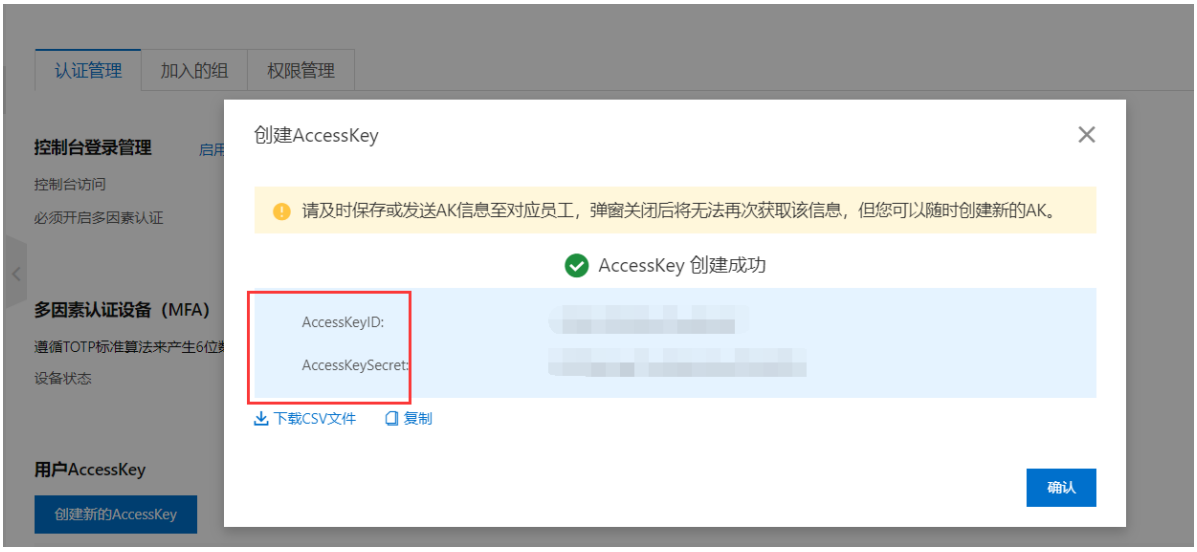
IDaaS应用身份服务通过RAM角色账户单点登录到阿里云控制台，拥有多个权限的RAM账户的员工，只需添加一个阿里云角色 SSO应用并将各角色账号添加到子账户中，即可实现阿里云中多个RAM角色的单点登录。

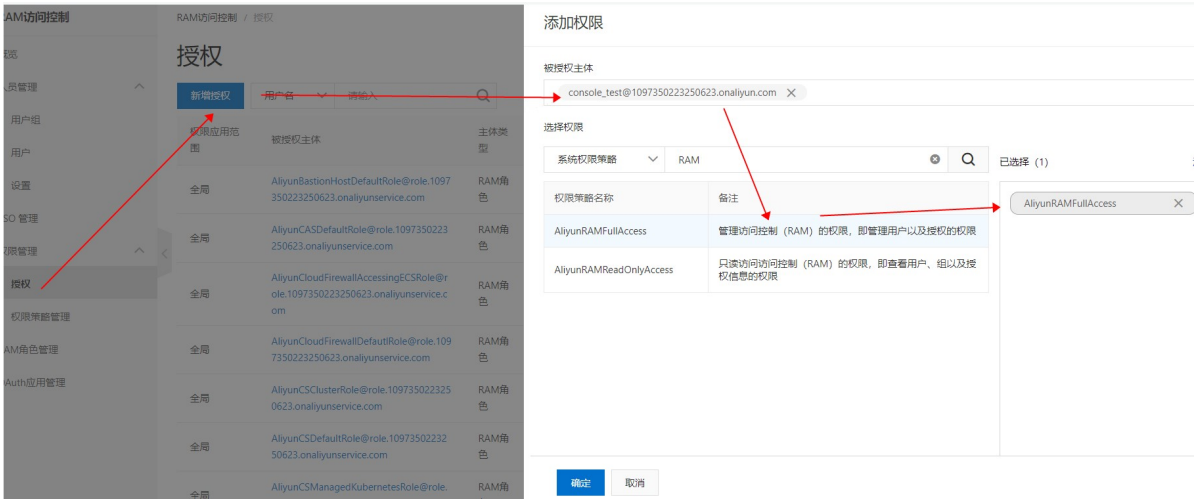
操作步骤

一、RAM账户准备

1. 添加用户
2. 点击左侧用户管理进入阿里云子用户列表，创建一个新用户或者任意选择一个已经存在的用户，点击进入页面



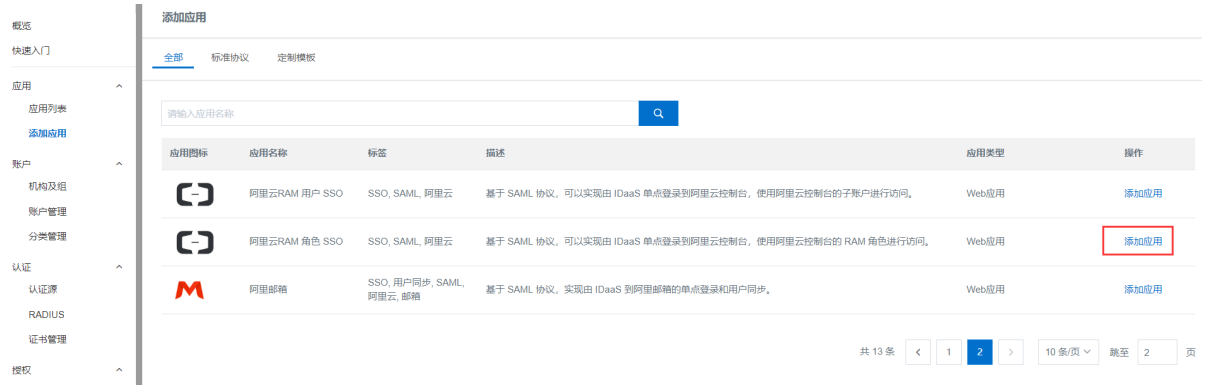
3. 获取AccessKeyID、AccessKeySecret，获取以后在IDaaS新建应用的时候需要填写，用于查询RAM角色列表。
4. 

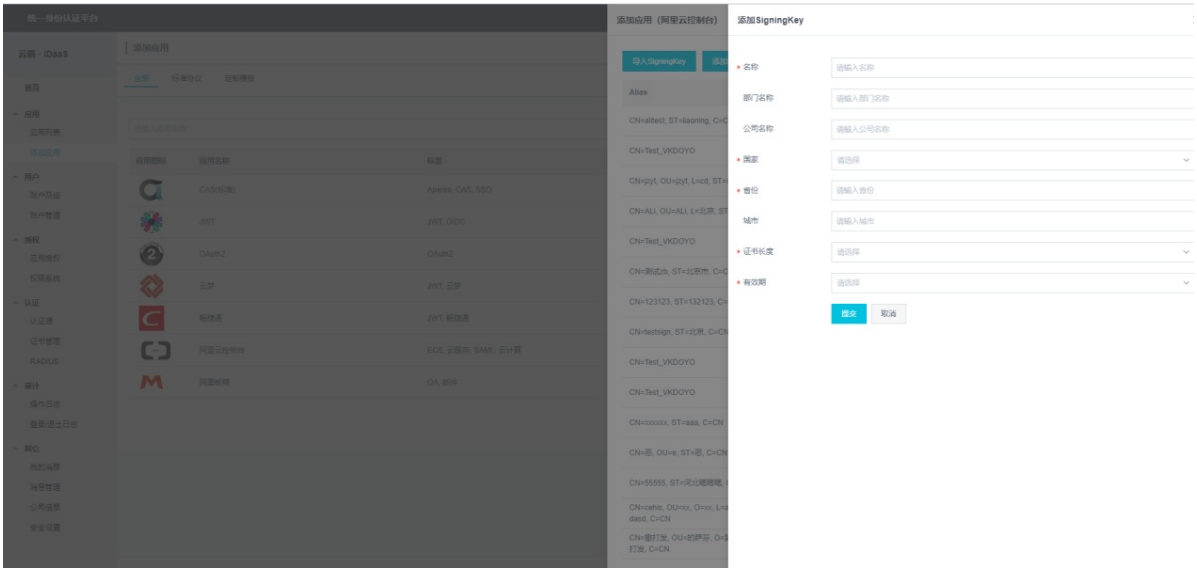
5. 给刚才创建的用户授权RAM所有控制权限AliyunRAMFullAccess
6. 

二、IDaaS添加阿里云控制台

1. 应用列表中选择阿里云控制台添加应用
2. 添加SigningKey(证书)

3.





4. 配置SAML内容

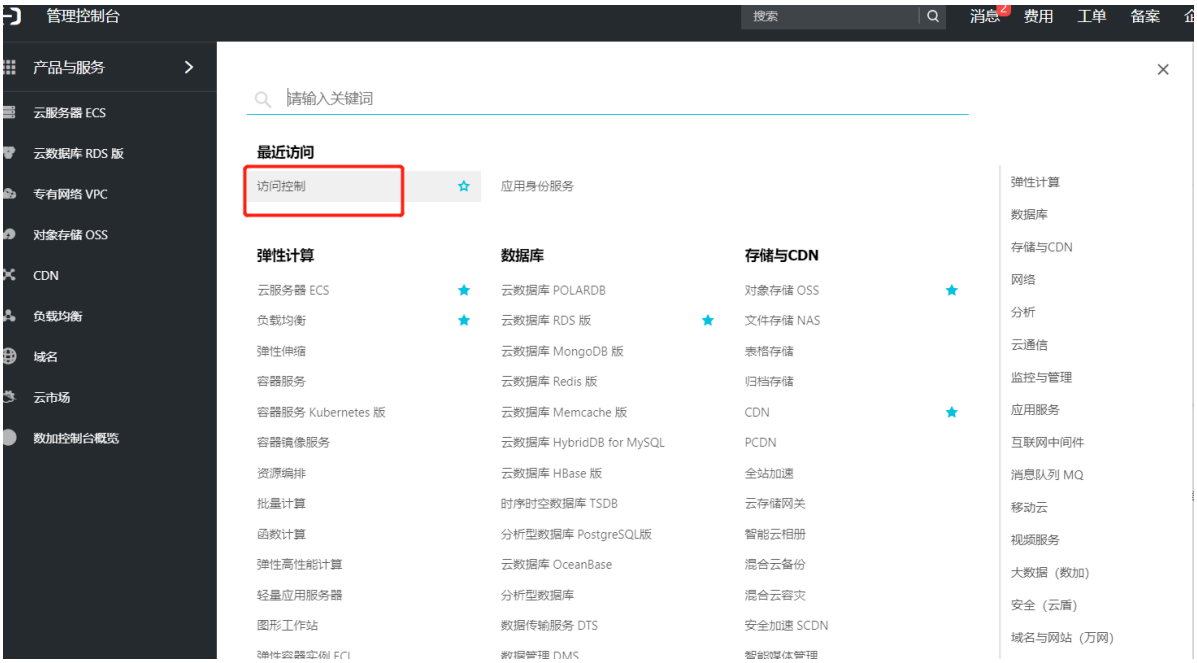
5. 在SigningKey列表界面中右侧点击“选择”进入SAML配置界面。根据提示填写DaaS IdentityId、SP Entity ID和SP ACS URL(SSO Location)等参数保存，都为默认值，其中阿里云个人域名称填写个人信息的用户ID,其中NameIdFomat选择"urm:oasis:names:tc:SAML:2.0:nameid-format:persistent"。

   下图是根据RAM用户信息内容进行的填写示例，其中必须要填写AccessKeyID、AccessKeySecret，该两个值由阿里控制台用户提供。

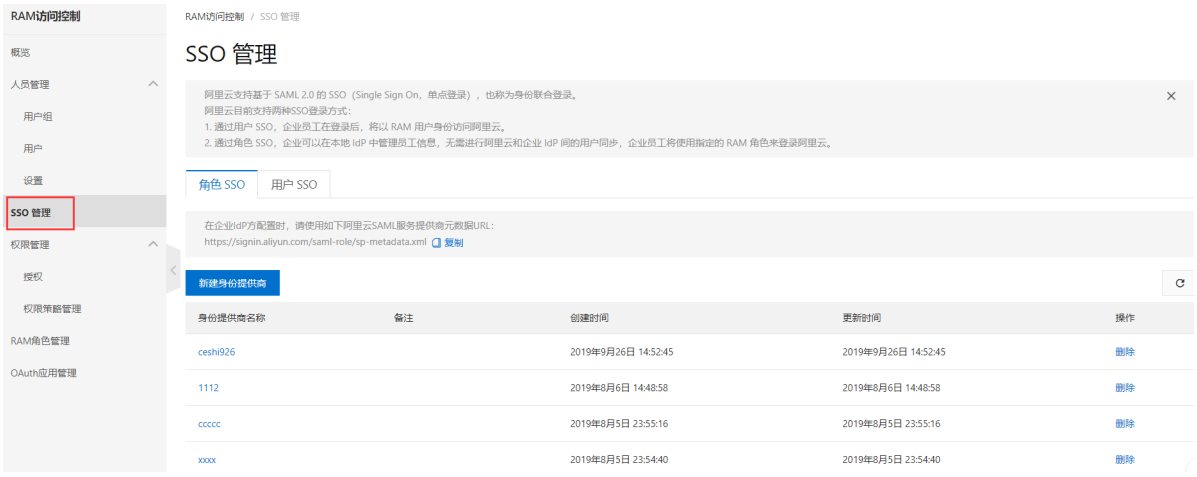
6. 保存应用成功，切换到应用列表，查看应用详情，导出SAML元数据文件Metadata.xml(在新建供应商的时候上传元数据文件)
7.

三、RAM中创建角色

1. 使用阿里云账号登录阿里云
2. 进入访问控制
3. 登录控制台->产品与服务->搜索访问控制->进入RAM访问控制

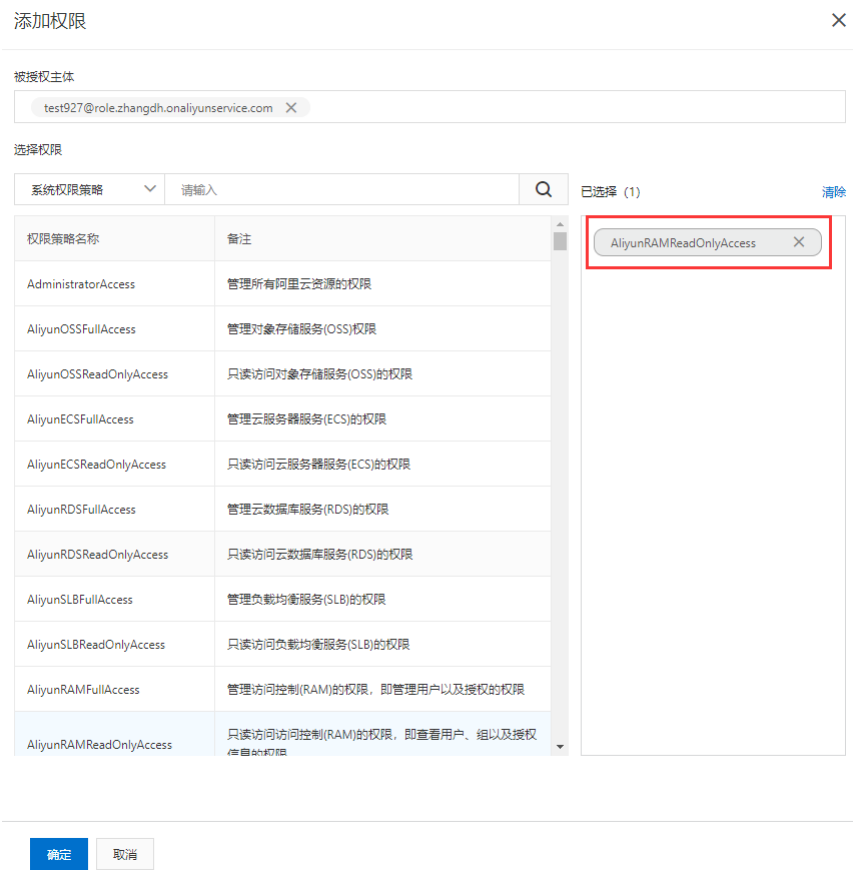


4. 新建身份提供商
5. 进入控制台后，点击SSO管理->新建身份提供商，并上传元数据文档（元文件由IDaaS提供，在下面IDaaS中创建应用处有下载步骤）提供商的名称任意填写。



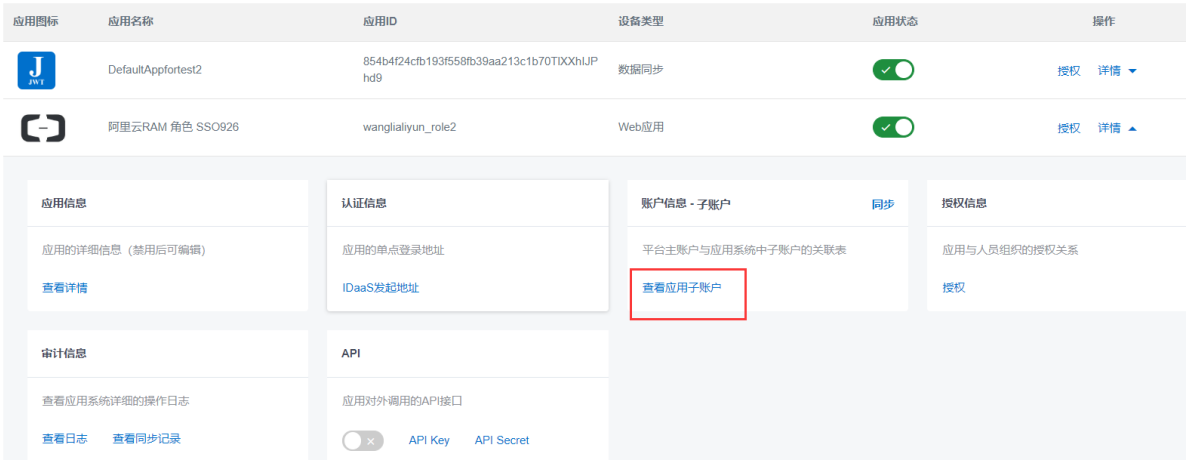
6. 新建RAM角色
7. 添加完身份提供商以后，点击“新建RAM角色”进入页面，角色名称任意填写，身份提供商可以任意选择已经有的。

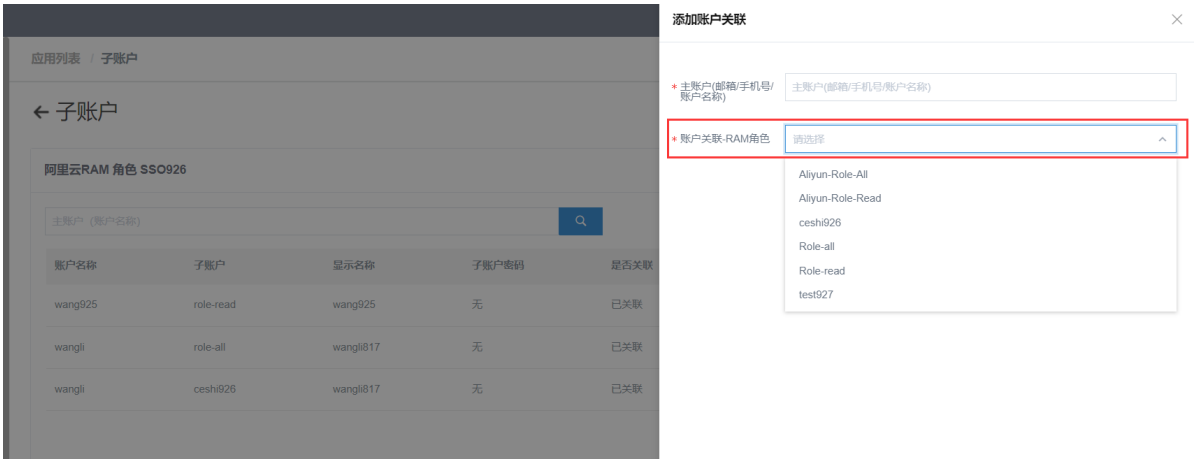
角色创建成功以后，需要为角色授权，点击“角色授权”进入页面,至少要给角色赋予访问控制查看的权限“AliyunRAMReadOnlyAccess”，若未赋予访问控制任何权限，则会提示“没有权限调用”。

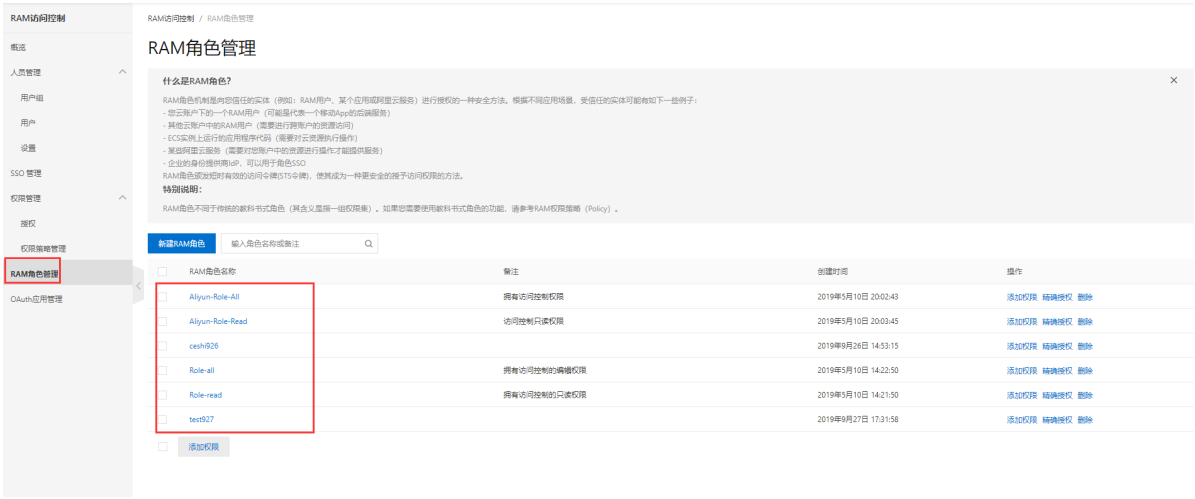


四、IDaaS配置子账户

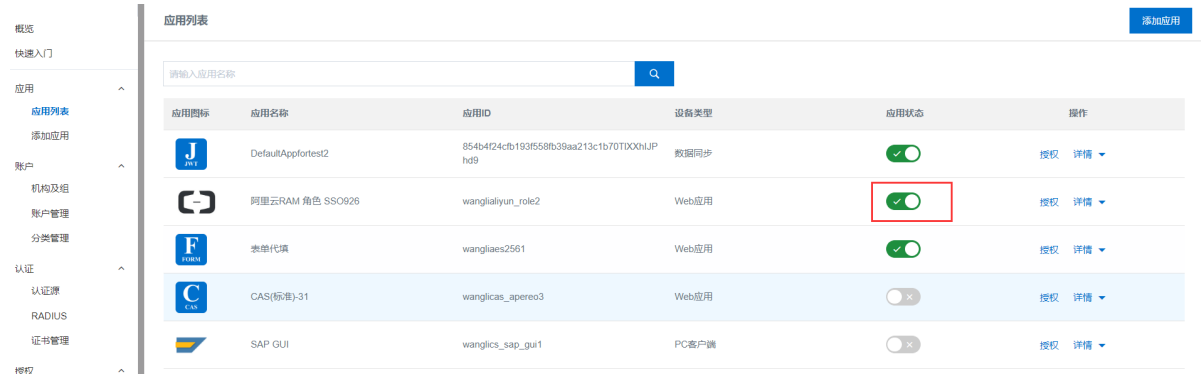
1. 可以在应用列表点击详情->查看应用子账户->添加应用子账户，下拉框展示的子账户是阿里控制台里面“RAM角色”，选择的子账户（RAM角色），必须是上传对应的元数据文档的角色RAM对应的身份提供商。
2.





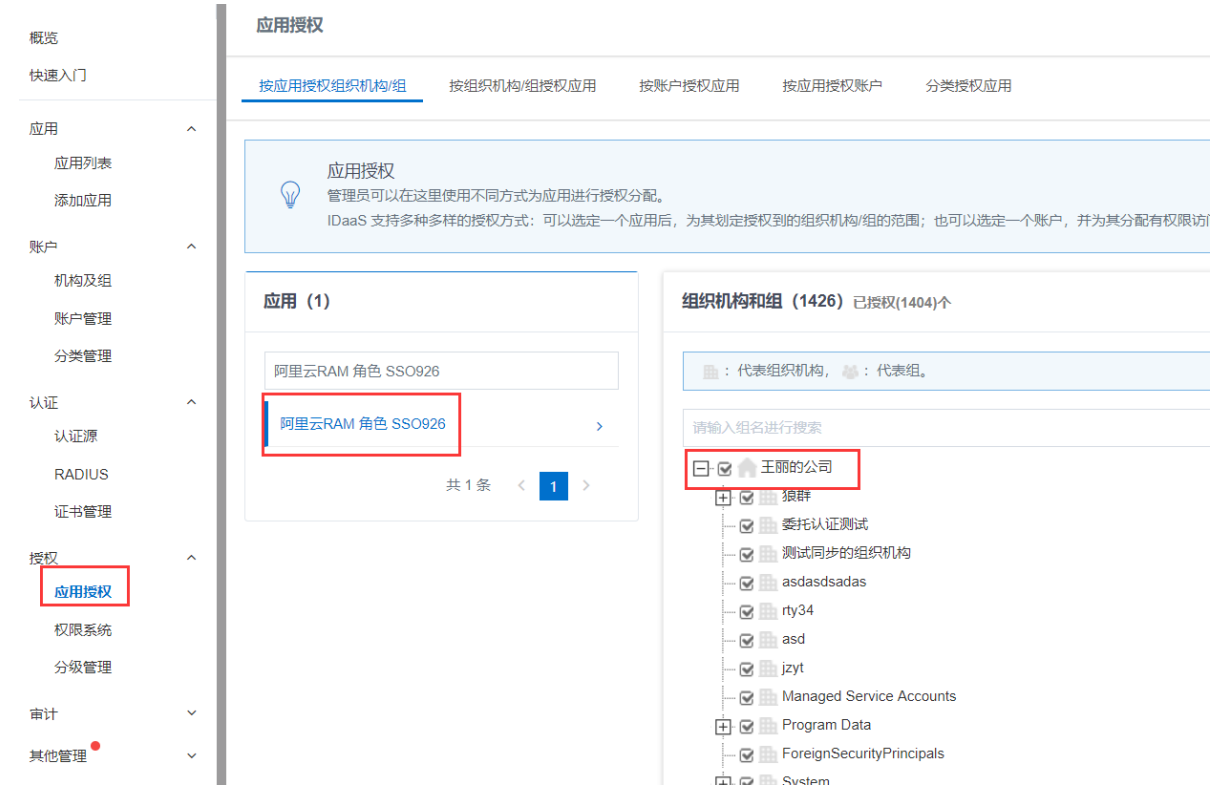


五、从IDaaS单点登录到阿里云控制台

1. 开启应用
2. 

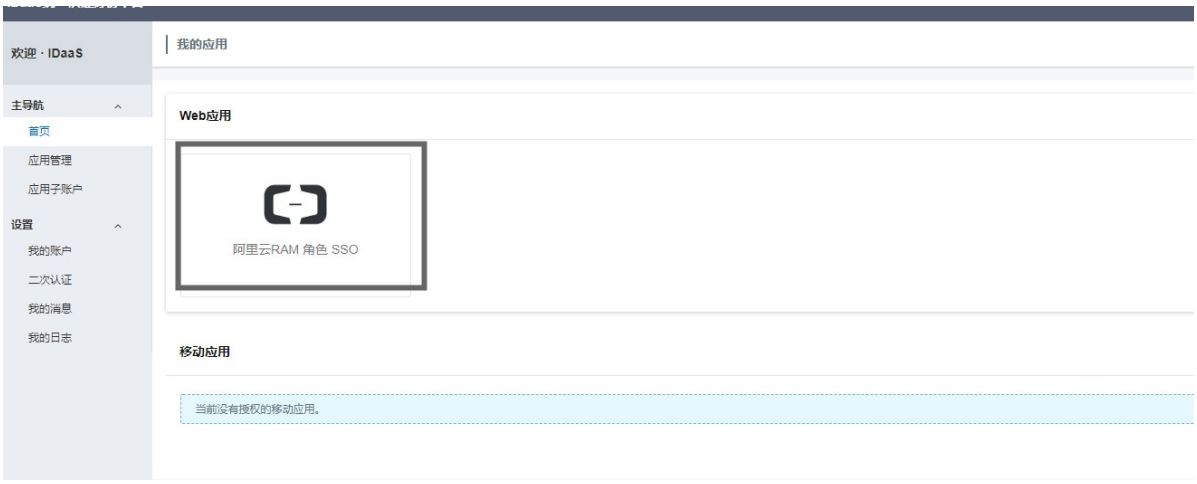
3. 在IDaaS中创建一个用户
4.

5. 在应用授权模块对应用进行授权
6.



7. 访问普通用户登录地址，copy下面的链接
8.

9. 输入IDaaS中创建的用户进行登录，登录成功后，点击首页的阿里云控制台图标进行单点登录
10.

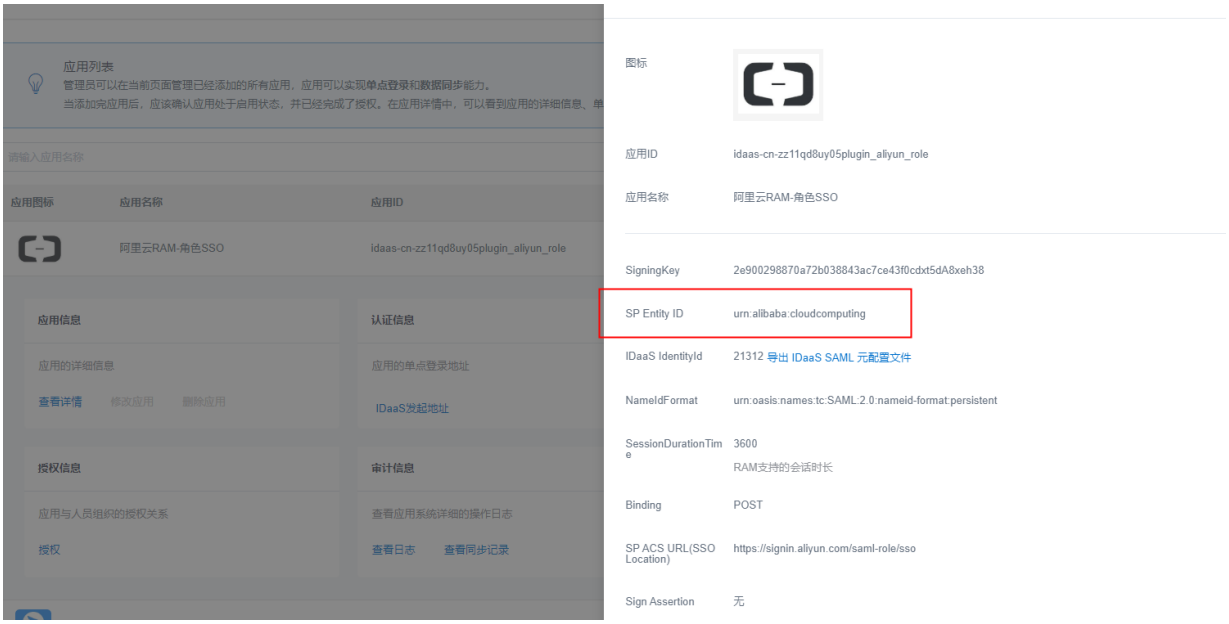


若以上步骤全部成功完成，即可实现RAM角色单点登录阿里云控制台。

FAQ

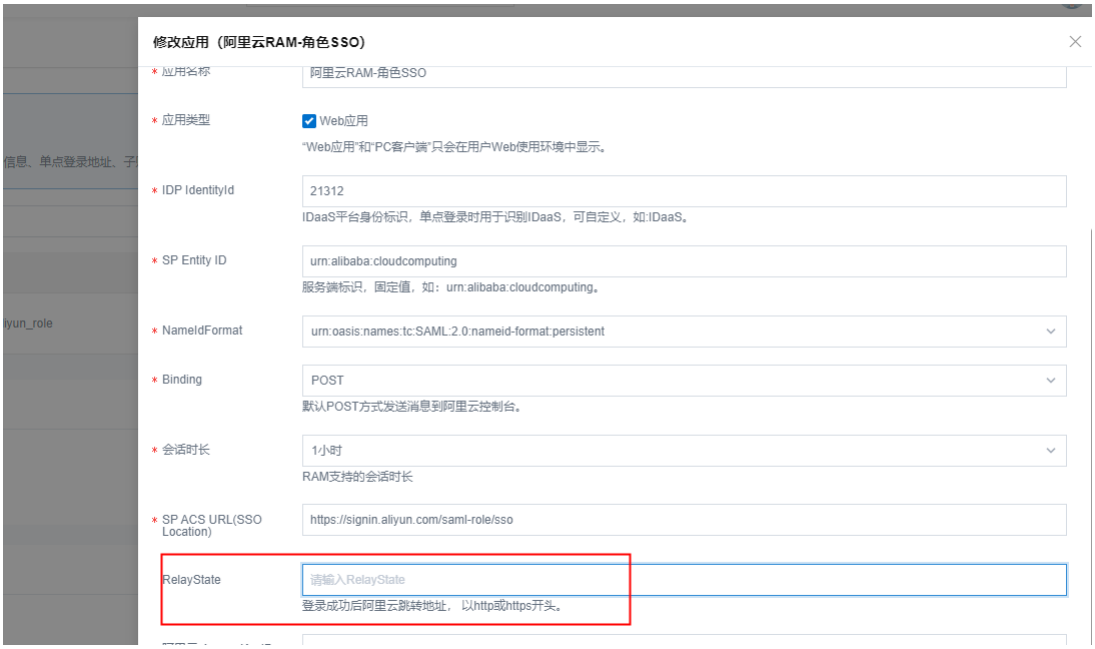
报错提示：
Can't find the intended audience in at least one nl

请参考下图，查看SP Entity ID 的值是否正确



如何修改SSO登录后跳转的地址？

修改RelayState的值



报错提示：Issuer invalidated by issuer value

IDaaS上配置的角色SSO，需要导出metadata文件在RAM上创建身份提供商，然后单点登录该身份提供商创建的角色。可以排查下，是否单点登录的角色不是该应用创建的身份提供商中提供的角色。

报错提示：Can't find the intended audience in at least one AudienceRestriction.

请检查IDaaS页面配置的角色SSO参数是否正确

报错提示：提示时间不匹配

在IDaaS中配置的SessionDurationTime和RAM中角色设置的最大会话时间不匹配，需要修改RAM中的最大会话时间。

1.3. IDaaS同步账户到RAM配置说明手册

本文为您介绍如何配置使IDaaS同步账户到阿里云RAM中，以实现两个平台的账户信息同步保持一致。

背景信息

在现代企业的数字化管理中，某些企业员工日常办公需要访问阿里云控制台，但应用系统之间账户并未同步，成为一个个信息孤岛，所有应用的数据同步难题，正困扰着越来越多的企业管理者。

解决方案

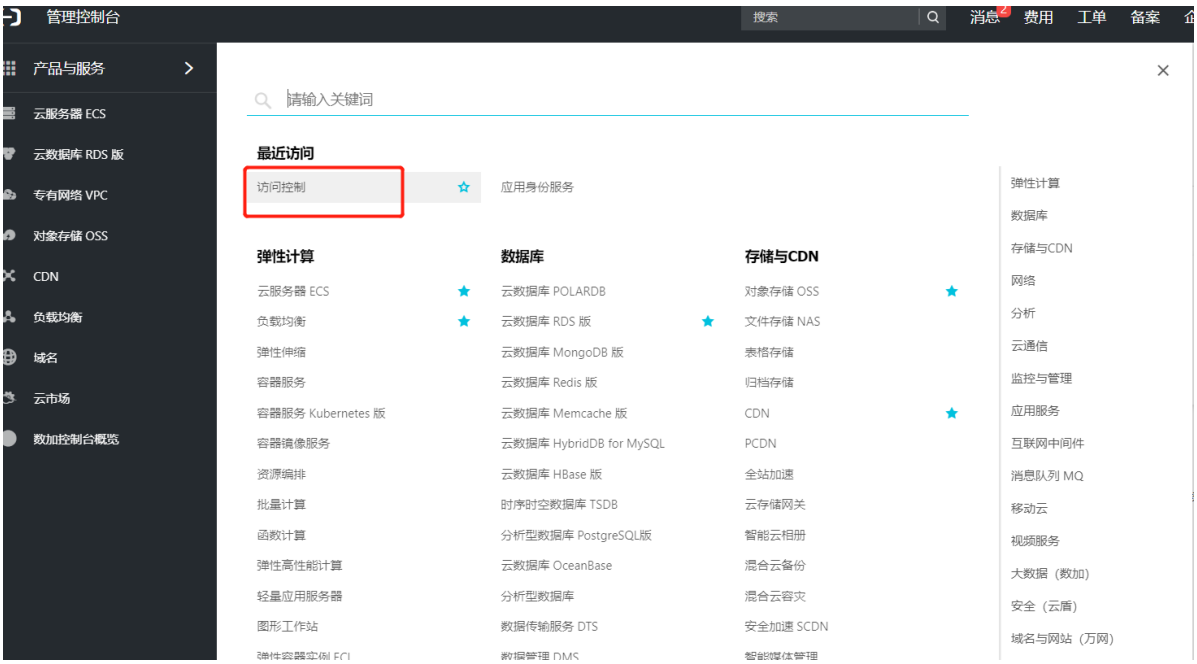
通过IDaaS应用身份服务的SCIM协议,将企业内部共享数据同步到阿里云RAM服务中去。

操作步骤

一、RAM账号准备

1. 使用阿里云账号登录阿里云
2. 进入访问控制

   登录控制台->产品与服务->搜索访问控制->进入RAM访问控制

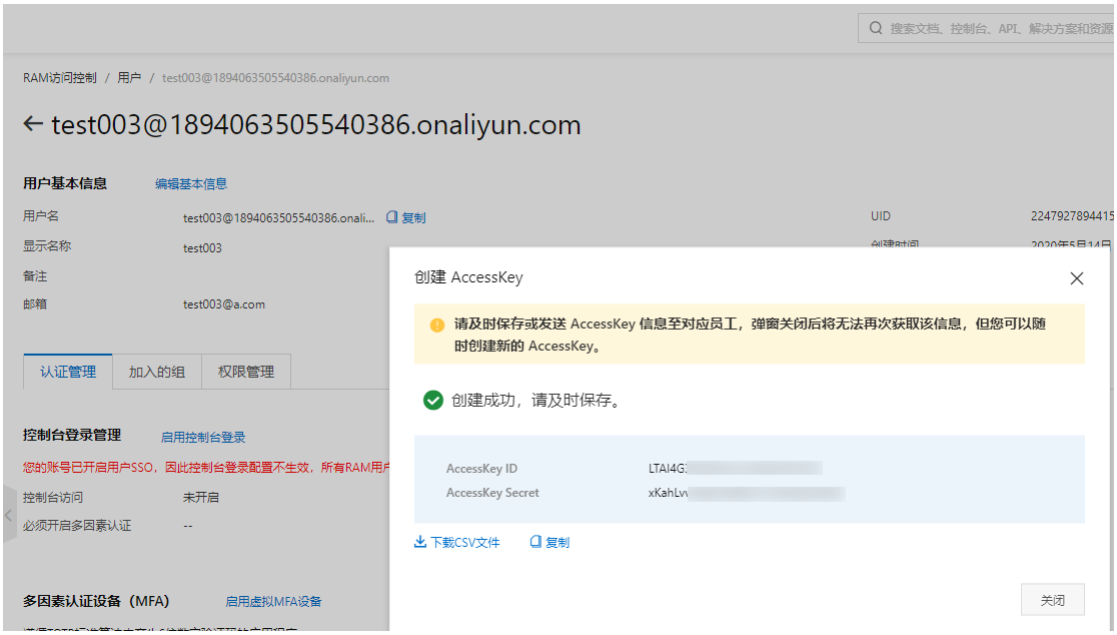


3. 添加用户

   点击左侧 **人员管理-用户** 进入阿里云用户列表，创建一个账户，如 test003，创建成功后在用户列表中可以看到该用户。

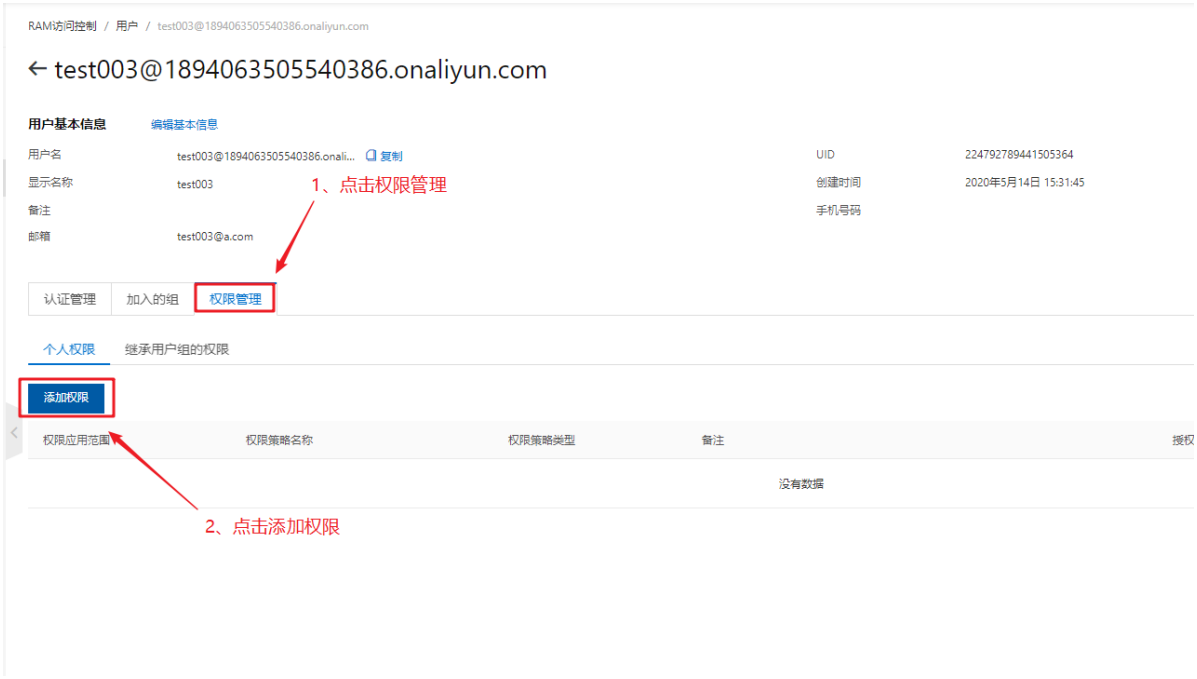
4. 点击账户名称进入账户详情页面，点击创建AccessKey

将生成 AccessKey ID 和 AccessKey Secret 安全保存到本地。

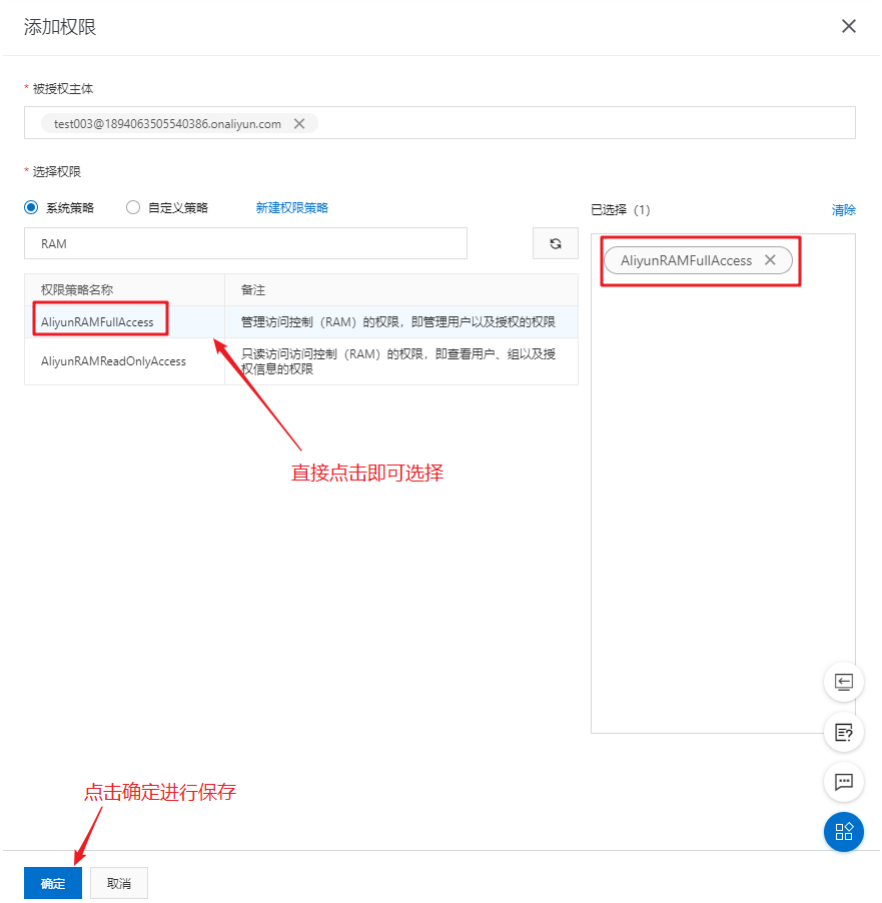


5. 给新用户设置管理RAM的权限（AliyunRAMFullAccess）

   切换到权限管理标签，点击添加权限

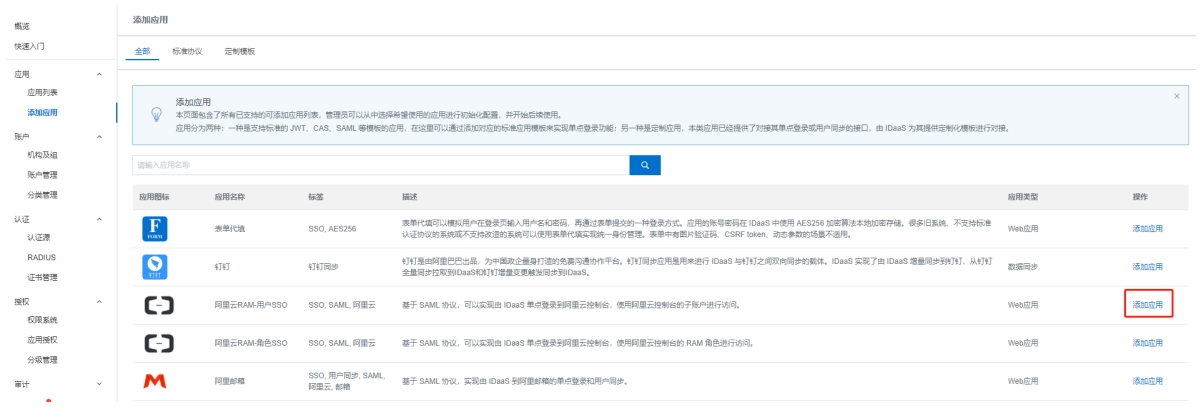


在搜索框中输入 RAM，即可快速找到 AliyunRAMFullAccess 权限策略。点击该策略，选上之后点击确定保存即可。

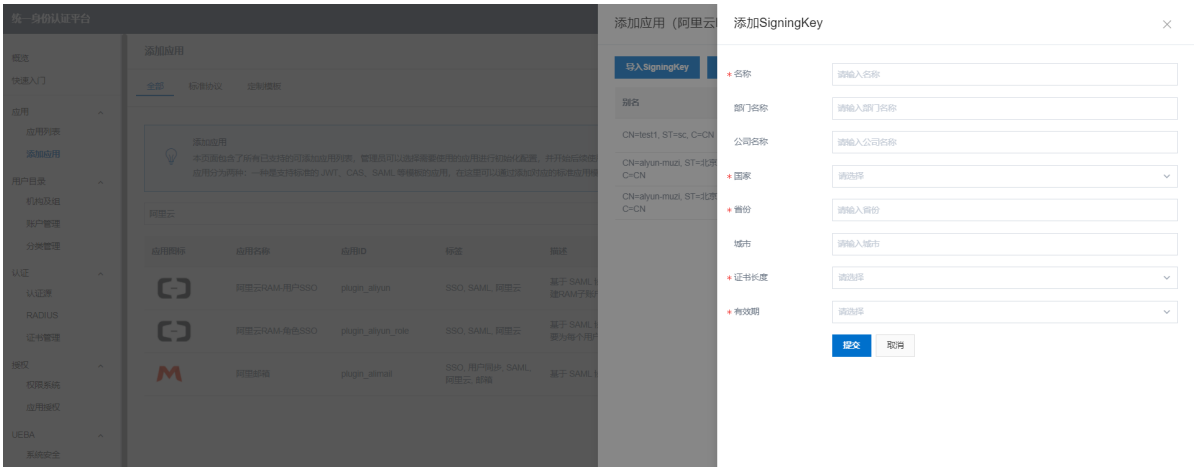


二、IDaaS添加阿里云控制台

1. **应用列表**中选择阿里云RAM-用户SSO添加应用



2. 添加SigningKey(证书)

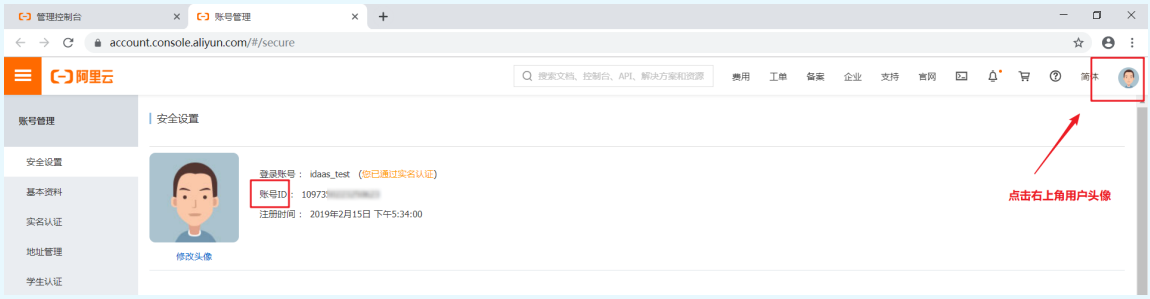


3. 配置SAML内容在SigningKey列表界面中右侧点击“**选择**”

   进入SAML配置界面。根据提示填写个人域名， identityId和SP identityId等参数保存。下图是根据RAM账号信息内容进行的填写示例：

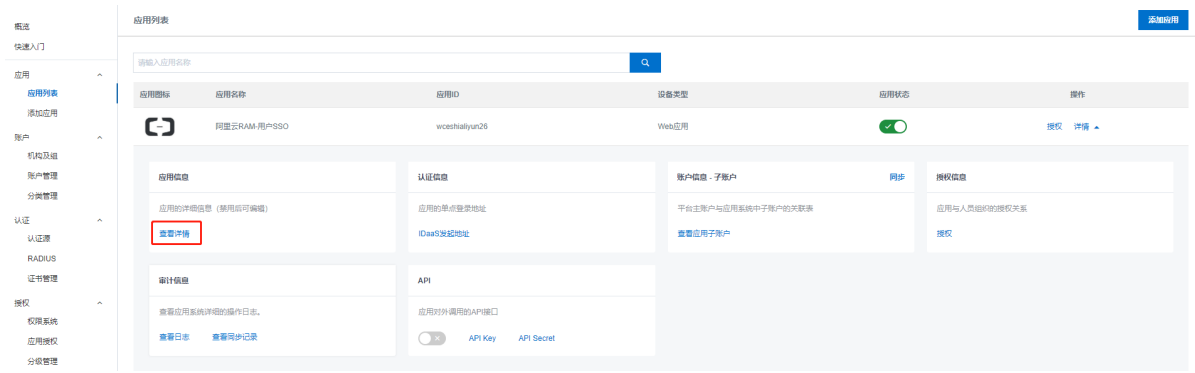
   - 阿里云个人域名称：例如1894063505540386.onaliyun.com，其中 1894063505540386 需要替换成阿里云账号ID
   - IDaaS IdentityId：例如 https://signin.aliyun.com/1894063505540386/saml/SSO，其中 1894063505540386 需要替换成阿里云账号ID

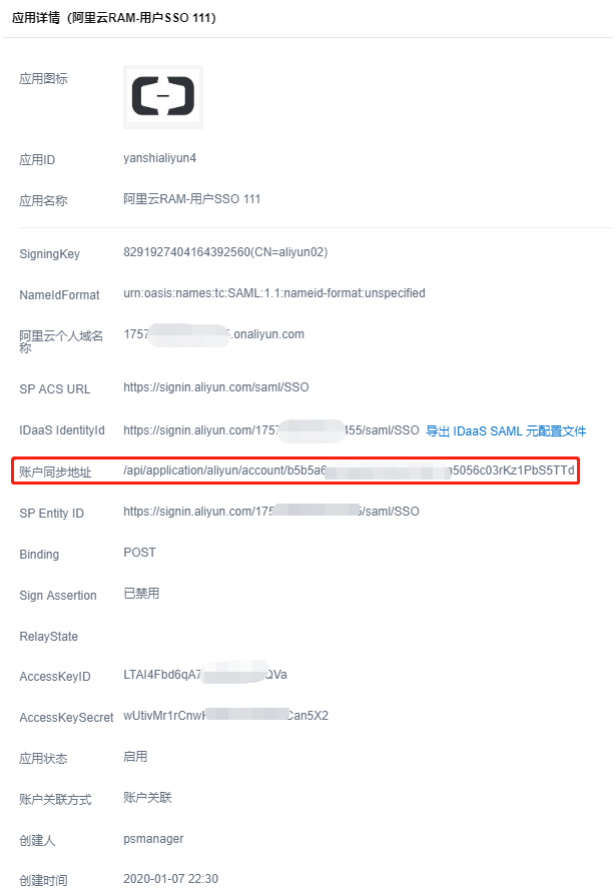
   > **说明**
   >
   > **阿里云账户ID** 获取方式如下：
   >
   > 在阿里云控制台点击右上角头像图标，在账号管理-安全设置页面获取阿里云账号ID



   - SP Entity ID：与IDaaS IdentityId保持一致
   - SP ACS URL(SSO Location)：https://signin.aliyun.com/saml/SSO
   - AccessKeyID和AccessKeySecret：第一步创建的阿里云账号的AccessKeys
   - NameIdFormat：urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
   - Binding：POST
   - SP登录方式：应用自定义登录页
   - 账户关联方式：账户关联

4. 保存应用成功，切换到**应用列表**，查看**应用详情**，将该应用的账户同步地址，安全保存在本地。



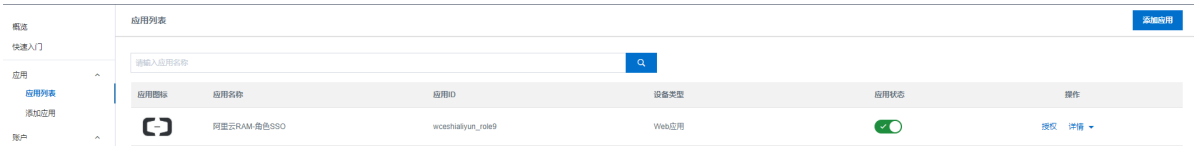


5. 获取用户账户同步接口认证的Key和Secret

   进入**应用列表 > 详情**，开启API开关，复制API Key和API Secret到本地进行安全保存。

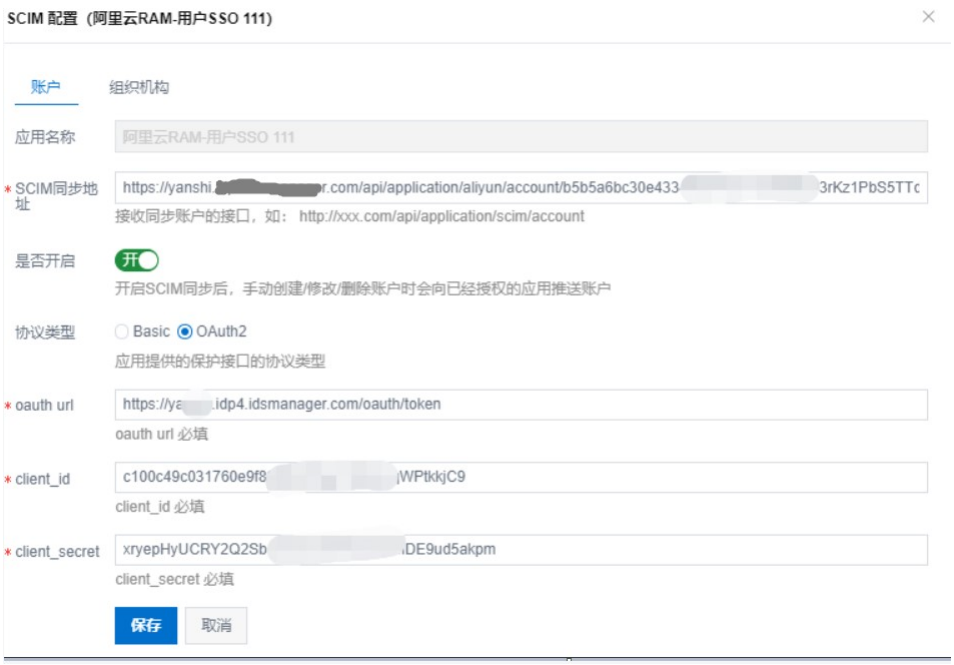
三、 在IDAAS中配置账户同步

1. 进入**应用 > 应用列表**，找到新建应用，并开启该应用。



2. 依次选择**详情 > 同步**

3. 点击**SCIM配置**链接，进入配置页面：



SCIM同步地址：当前IDaaS域名地址+第二部分第4步获取的账户同步地址

> **注意** 地址中间没有空格，如果提供的接口开头有：openapi/2020-x-x,需要把这部分内容去掉

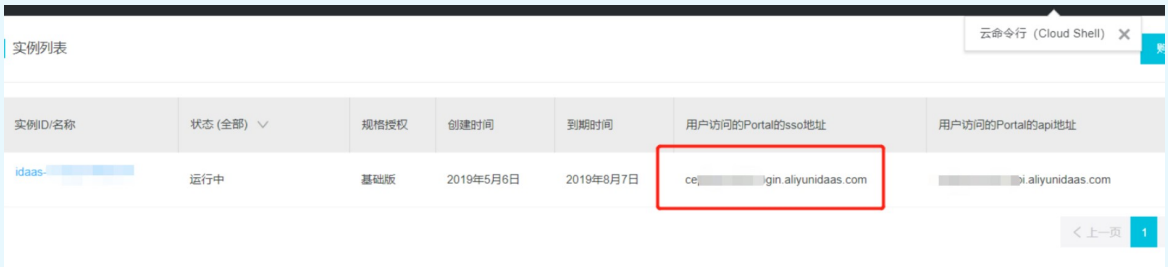
是否开启：开启此开关

协议类型：选择OAuth2

oauth url：当前IDaaS域名地址+/oauth/token

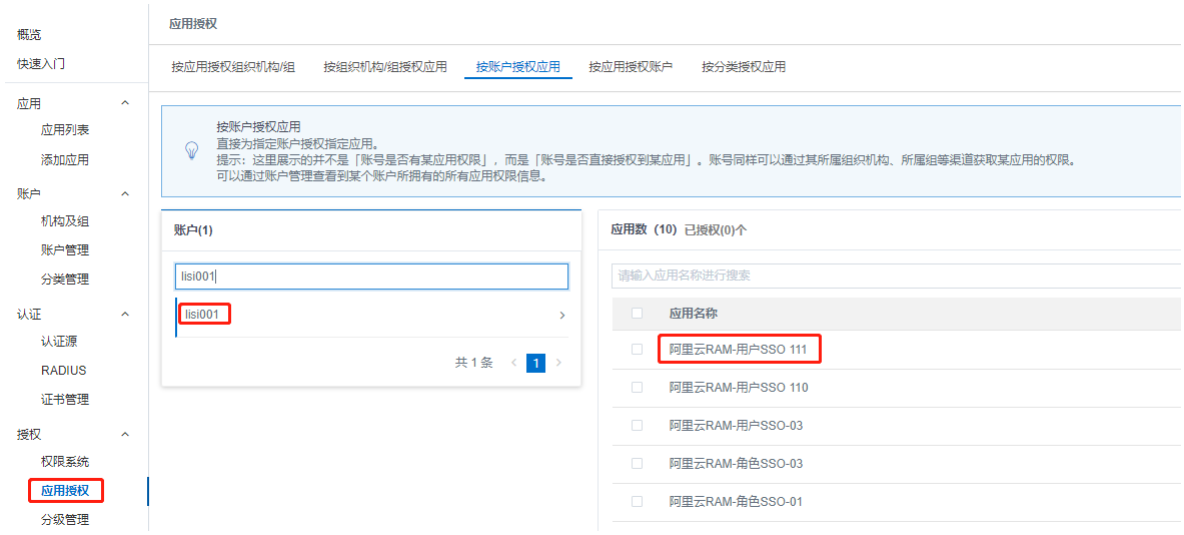
client_id和client_secret：第二部分第5步获取的API Key和API Secret

> **说明** IDaaS域名地址可以在云盾IDaaS管理控制台获取。



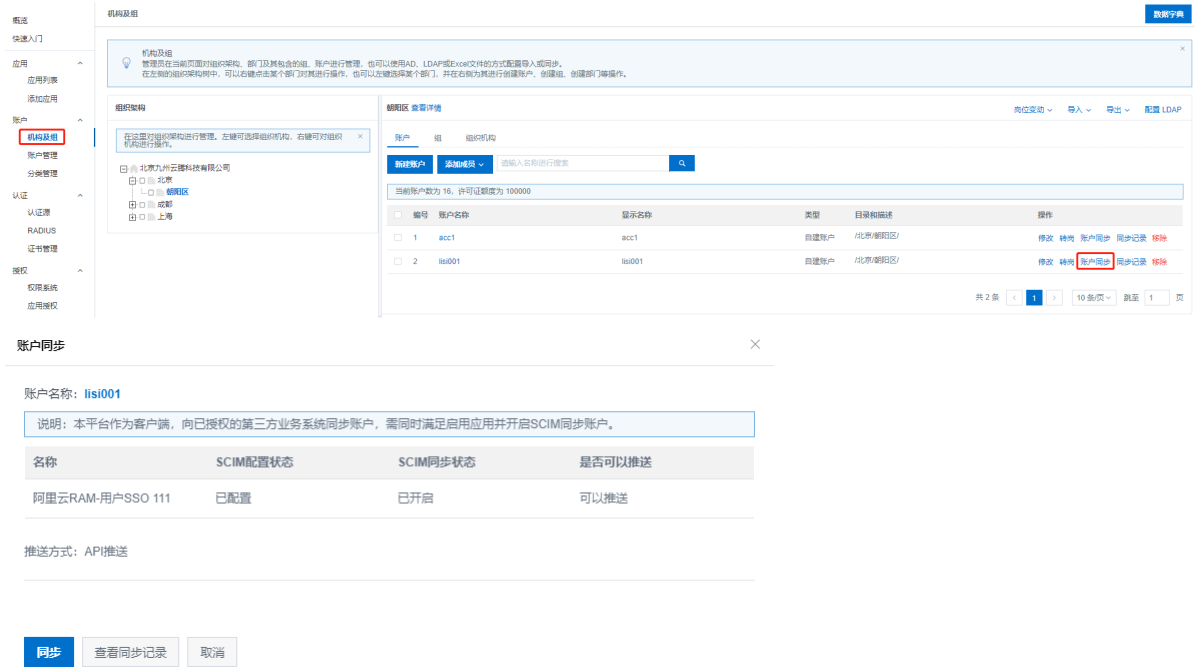
4. 在IDaaS中创建一个用户

5. 在**应用授权**模块对新应用进行授权



6. 账户同步进RAM

   进入**账户 > 机构及组**，找到刚新增的账户，选择账户同步链接



   选择**同步**按钮完成同步。

   点击**同步记录**查看同步结果：

7. 阿里云控制台中查看同步过来的账户

   切换到阿里云控制台中：**人员管理 > 用户**菜单，人员列表中可查看到新同步过来的账户：

   注意：以上步骤中有需安全保存到本地的关键信息，配置完成后请示情况进行安全删除。

1.4. IDaaS 打通 RAM 与 AD/钉钉扫码 等认证的集成

通过 IDaaS 认证能力，快速实现将 AD、钉钉扫码等认证方式集成用于登录阿里云RAM的效果。

概述

背景信息：

1. 客户的员工登录阿里云控制台时，只能单独在 RAM 中新建用户，而无法与现有身份目录 AD 集成联动，造成云上身份孤岛问题，增加了维护成本和安全风险，用户也需要多记一套账密；
2. 目前钉钉扫码，微信扫码，支付宝扫码等认证方式无法直接和RAM进行集成， 客户无法选择适合自身的认证方式登录阿里云控制台。

解决方案：

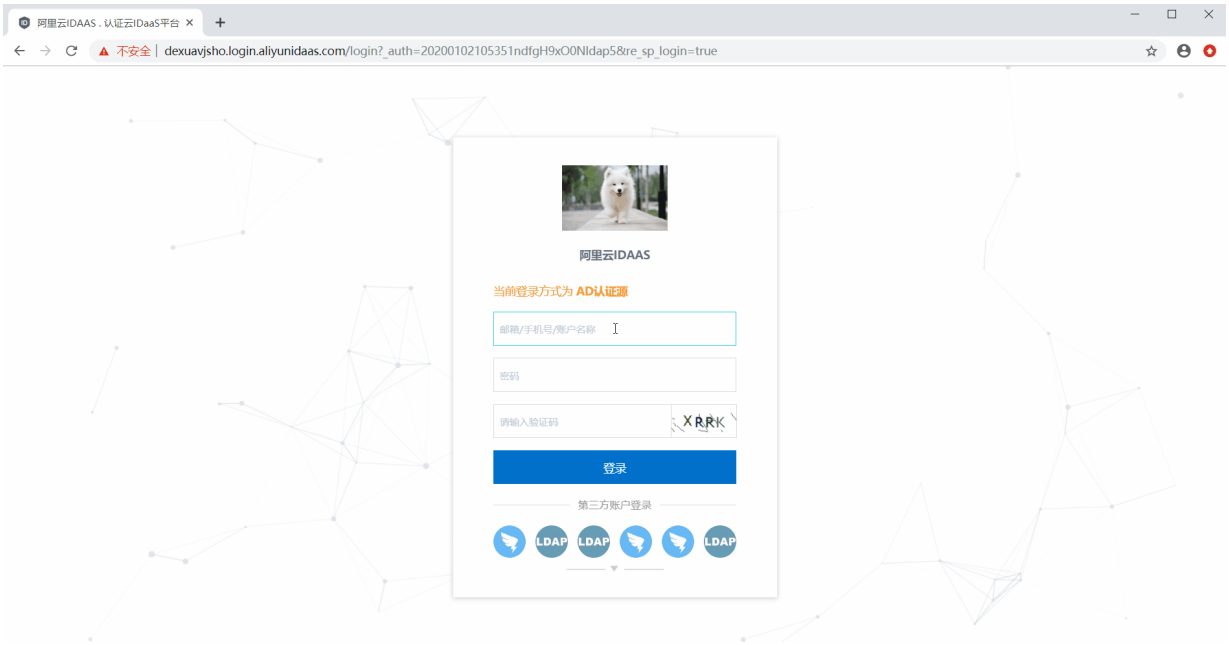
1. IDaaS支持常用的认证方式，如：AD账户和密码，钉钉扫码，微信扫码和支付宝扫码等，提供方便快速的对接流程。
2. 客户通过选择IDaaS提供的认证方式进行自助操作，配置完成后就可实现该认证方式登录RAM系统的目的。

收益：

1. IDaaS提供对接文档，操作简单，对接快速，减少自我研发对接认证方式的成本；
2. 客户只需一套账户体系，就可畅通访问RAM系统和其它应用，减少多套账户维护成本；

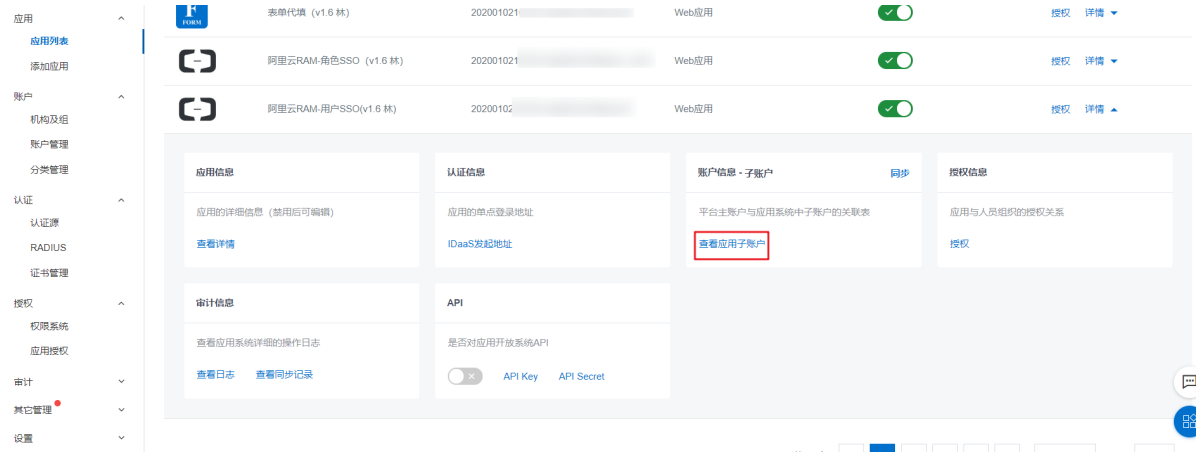
使用 AD 账户密码登录 RAM

效果演示

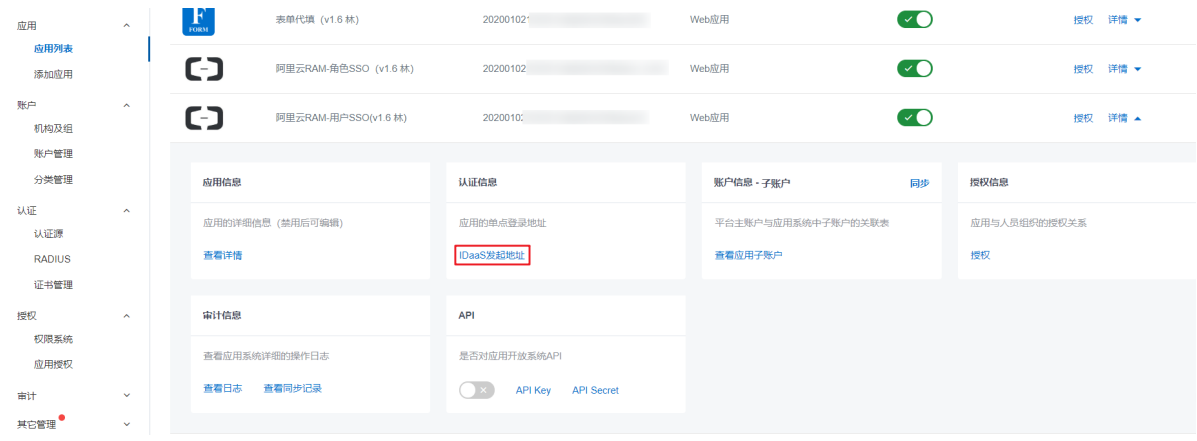


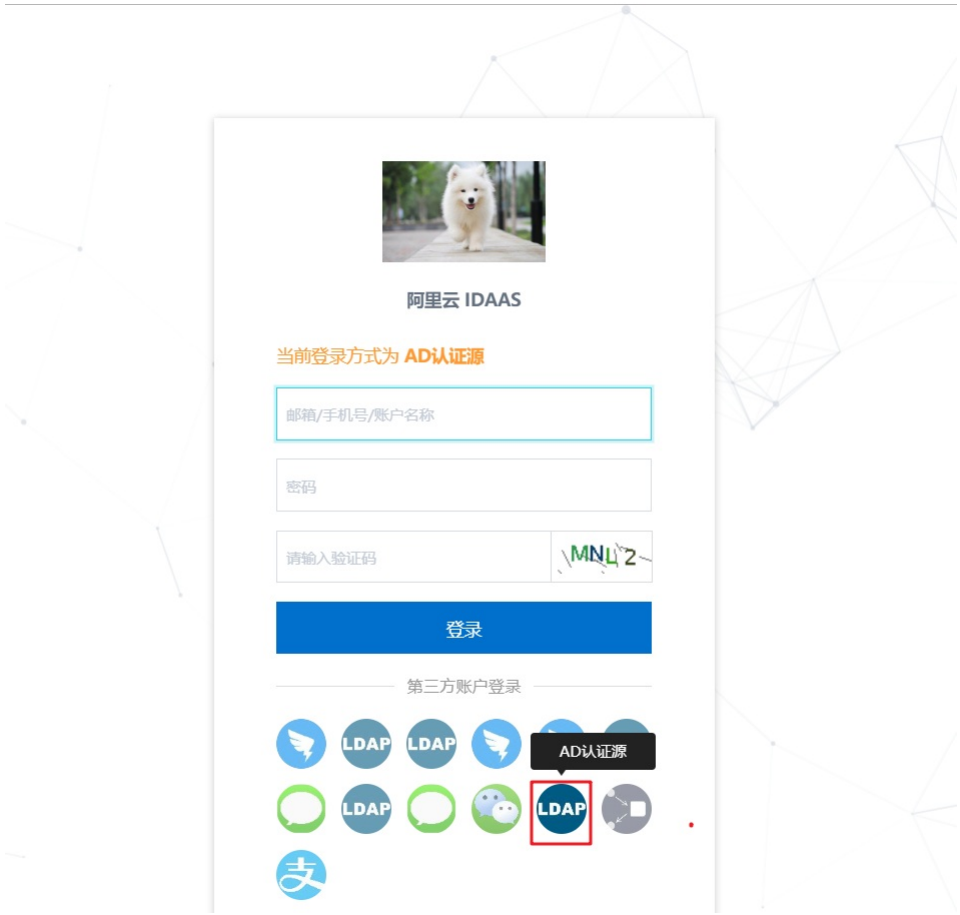
操作步骤

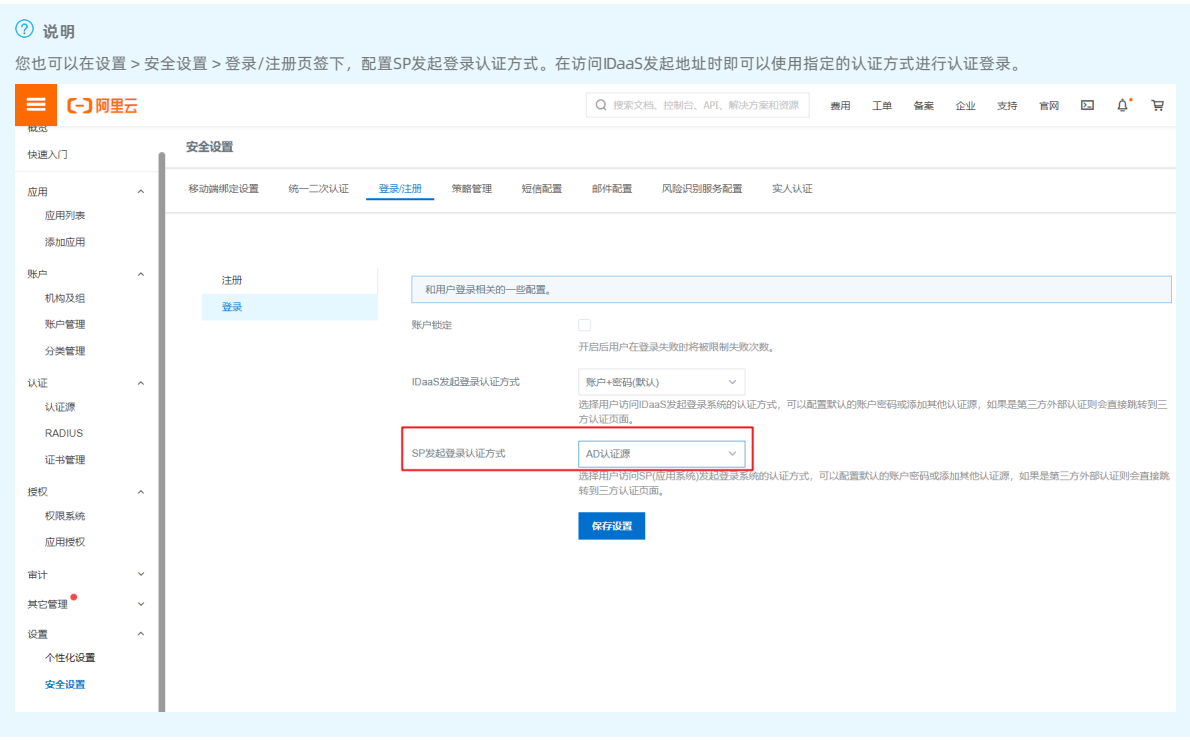
1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 配置添加AD认证源，操作步骤参考LDAP认证源使用手册。
3. 创建阿里云用户SSO应用，操作步骤参考使用RAM用户单点登录阿里云控制台。
4. 在**账户 > 机构及组**中新建LDAP同步配置，并将AD中的账户拉取到IDaaS平台，操作步骤参考 LDAP账户同步配置。
5. 在应用 > 应用列表中，选择步骤3中创建的应用。点击查看应用子账户，创建IDaaS账户与RAM的账户关联。



6. 浏览器访问应用的 IDaaS发起地址，选择AD认证源，输入AD中的账户密码即可实现使用AD账户密码认证登录到阿里云RAM

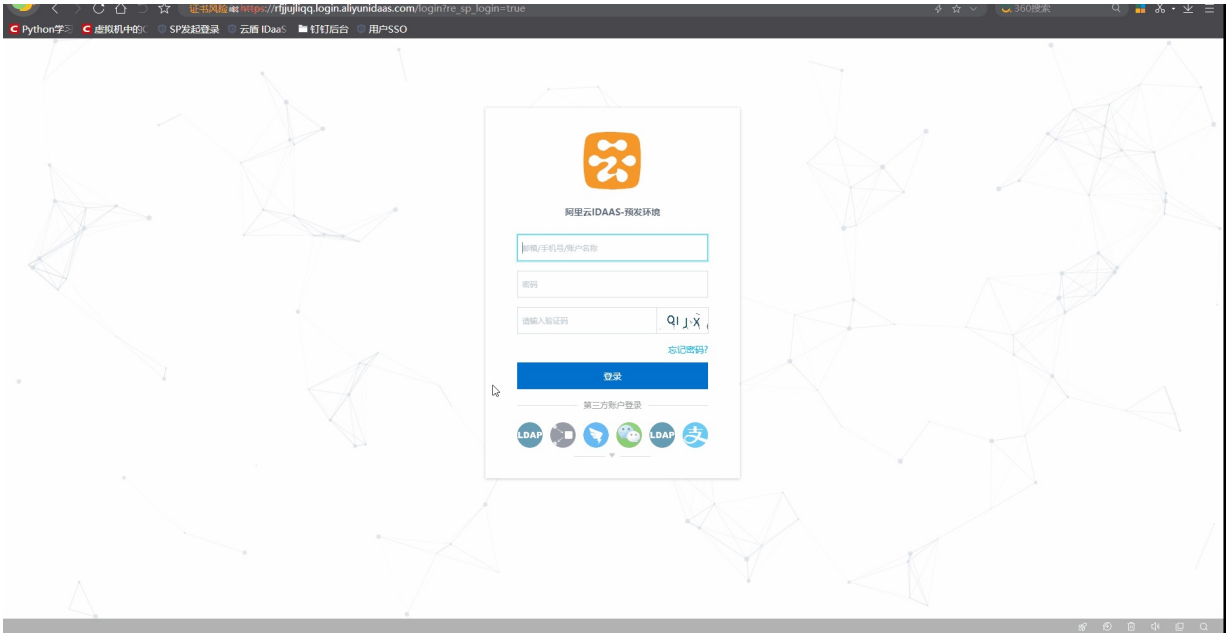

应用
应用列表
添加应用
账户
机构及组
账户管理
分类管理
认证
认证源
RADIUS
证书管理
授权
权限系统
应用授权
审计
其它管理
表单代填（v1.6 林）
阿里云RAM-角色SSO（v1.6 林）
阿里云RAM-用户SSO(v1.6 林)
Web应用
授权
详情
应用信息
应用的详细信息（禁用后可编辑）
查看详情
认证信息
应用的单点登录地址
IDaaS发起地址
账户信息 - 子账户
同步
平台主账户与应用系统中子账户的关联表
查看应用子账户
授权信息
应用与人员组织的授权关系
授权
审计信息
查看应用系统详细的操作日志
查看日志
查看同步记录
API
是否对应用开放系统API
API Key
API Secret


阿里云 IDAAS
当前登录方式为 AD认证源
邮箱/手机号/账户名称
密码
请输入验证码
登录
第三方账户登录
AD认证源
LDAP



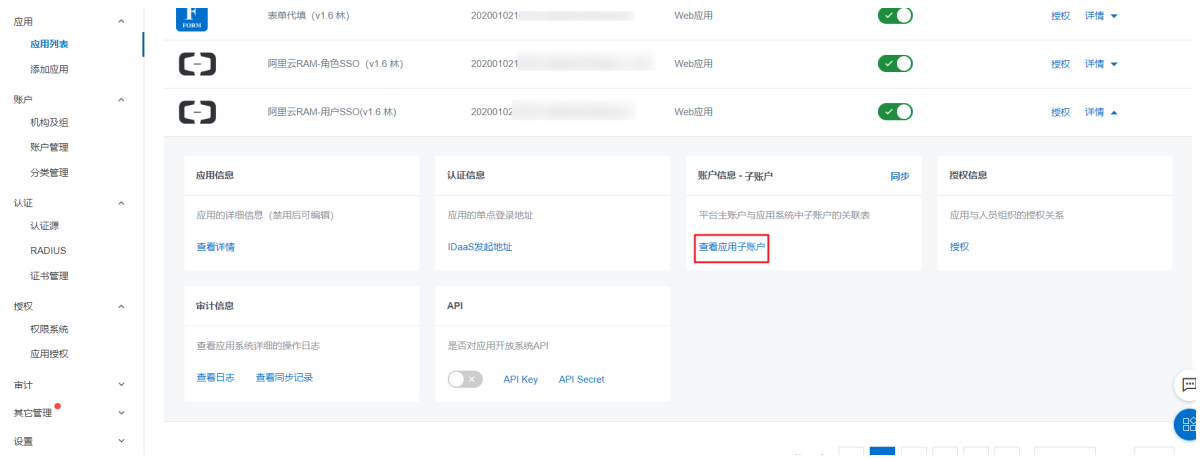
使用钉钉扫码登录 RAM

效果演示

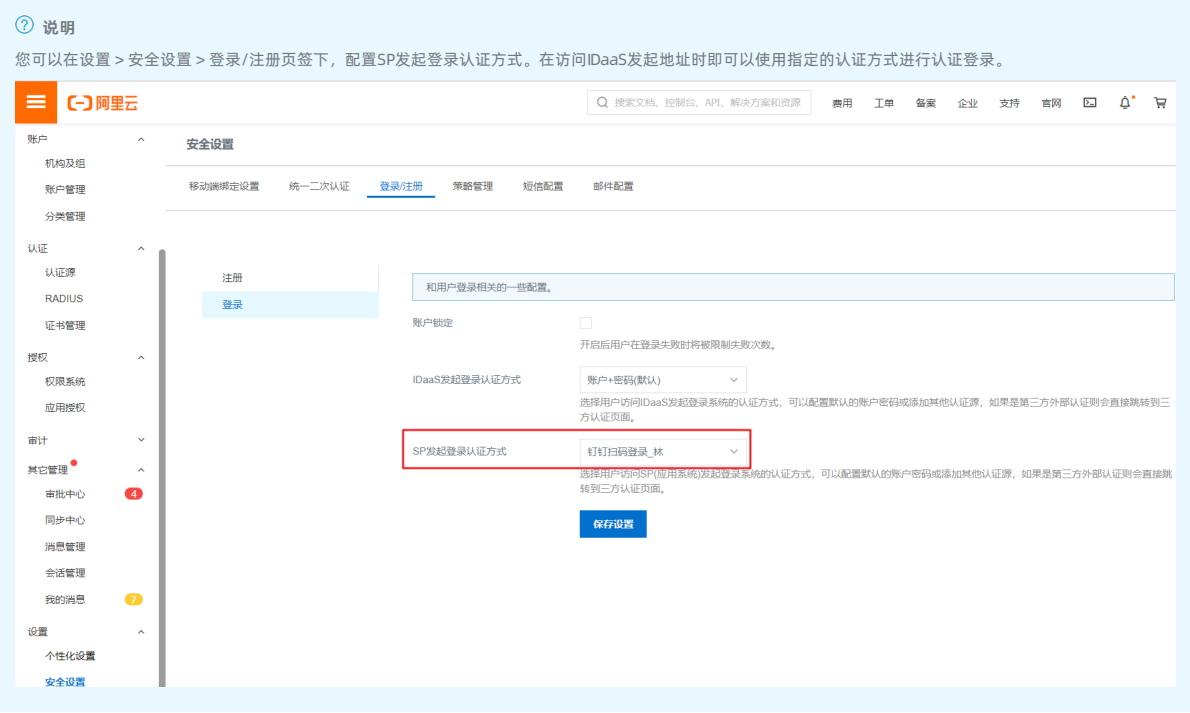


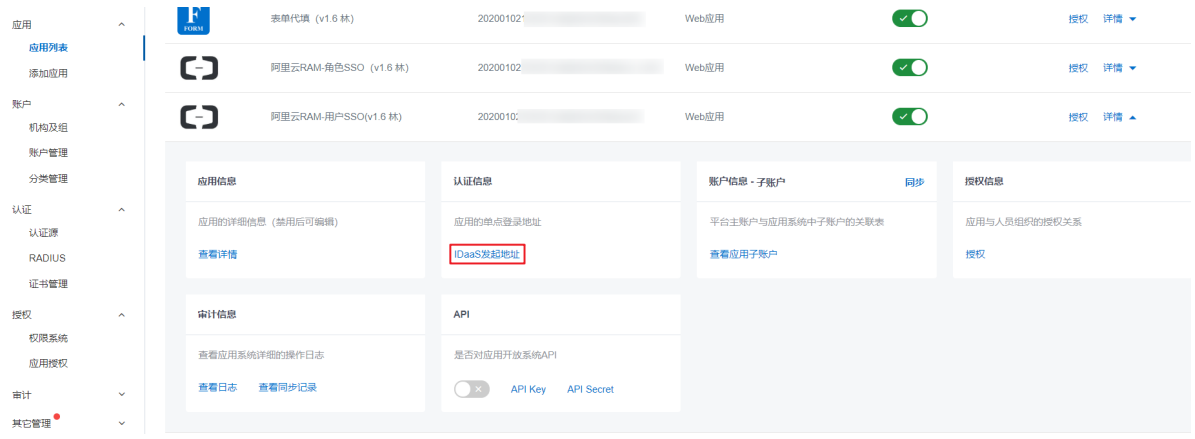
操作步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 配置添加钉钉扫码认证源，操作步骤参考配置钉钉扫码认证源
3. 创建阿里云用户SSO应用，操作步骤参考使用RAM用户单点登录阿里云控制台
4. 在应用 > 应用列表中，选择步骤3中创建的应用。点击查看应用子账户，创建IDaaS账户与RAM的账户关联。



5. 浏览器访问应用的 IDaaS发起地址，选择钉钉扫码认证源，即可实现使用钉钉扫码认证登录到阿里云RAM






阿里云IDAAS-预发环境
邮箱/手机号/账户名称
密码
请输入验证码
忘记密码?
登录
钉钉扫码登录_林
LDAP
LDAP
LDAP

2.单点和同步数据到阿里邮箱

本文为您介绍如何通过IDaaS应用管控功能，帮您实现阿里云邮箱的单点登录以及企业数据变更的同步。

背景信息

某些公司将阿里云邮箱作为企业的专用邮箱，日常工作中，阿里云邮箱作为企业内部员工、合作伙伴、供应商以及客户之间的沟通应用，登录频次高且要求数据实时更新同步。

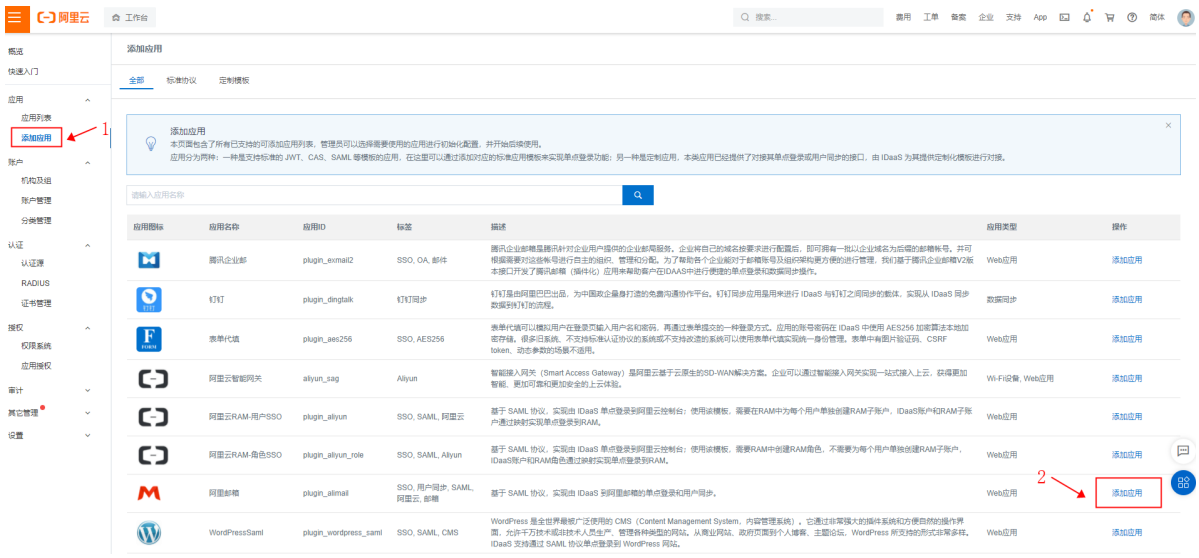
- 阿里云邮箱使用频次高，登录繁琐且耗时长。
- 在员工离职、合作终止等情况发生时，如果信息同步不及时，邮箱权限收回不及时，易造成公司信息泄露等风险；

解决方案

通过应用身份服务的应用管控（Application）功能，集中管控阿里云邮箱，实现快捷的单点登录并实时同步企业数据。

操作步骤

1. 新增阿里邮箱应用并进行配置



其中，appCode,appSecret 用于单点登录，accessCode ,accessPassword 用于组织机构及账户的接口同步。

以上四个值需向阿里邮箱相关同学（可以工单咨询阿里邮箱）进行申请（通过邮件申请）。

同时，需要把服务器的出口IP提供给阿里邮箱的工作人员，并将其添加到阿里邮箱的白名单后才可以进行正常数据同步。

公司邮箱域名：http:/

公司名称：

申请测试环境域名：http://

目前测试环境的出口ip:

需要访问的接口：账户及组织架构同步

单点登录： 需要 appCode, appSecret

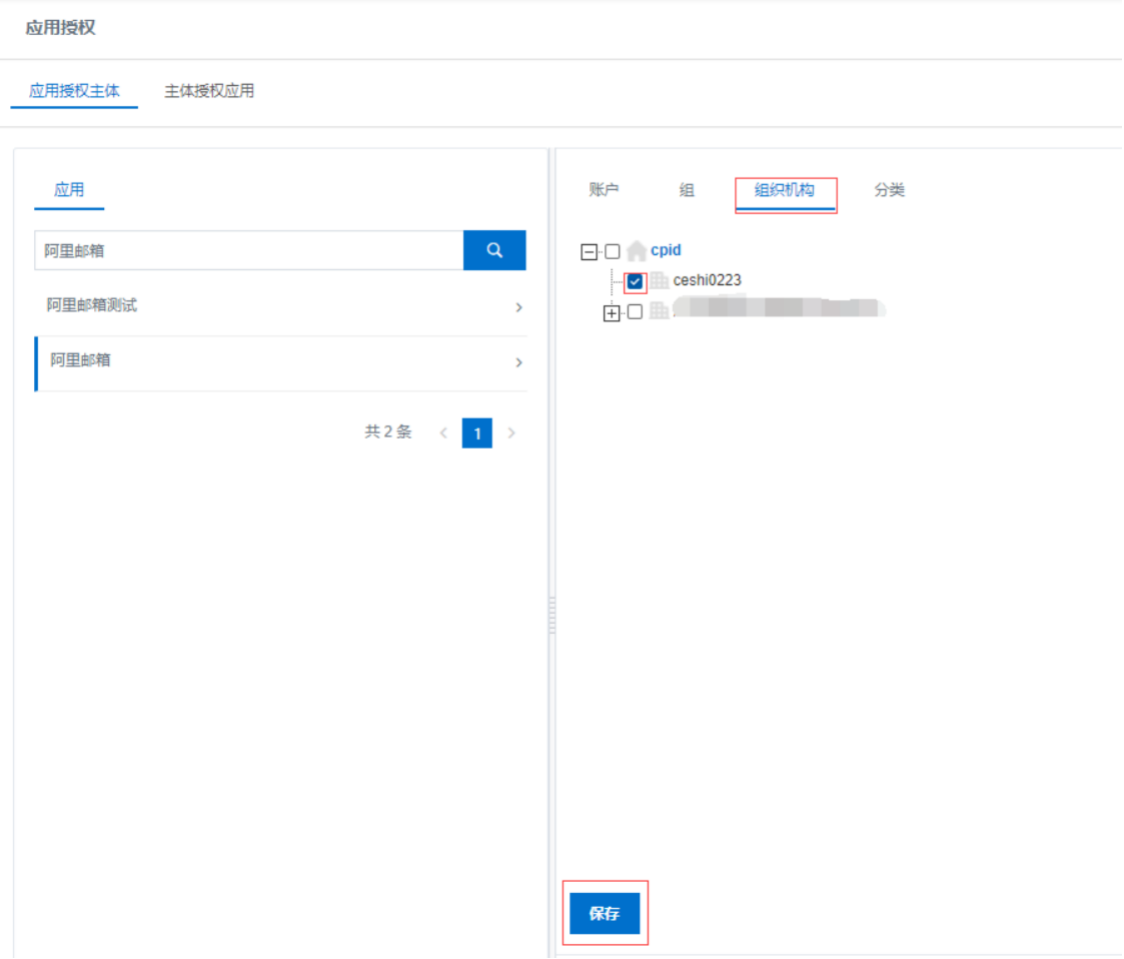
访问接口： 需要 accessToken ，accessTarget

“本系统根OU外部id”为IDaaS的root OU的外部id，管理员可以在账户及组中点击root OU的“查看详情”中获取。

2. 启用阿里邮箱应用并查看详情，获取同步组织机构和账户的地址 。

3. 启用阿里邮箱应用详情中的API，并获取APIKey和APISecret 。

4. 把该阿里邮箱应用授权给组织机构，组织机构下的用户就可以获得该应用的权限。

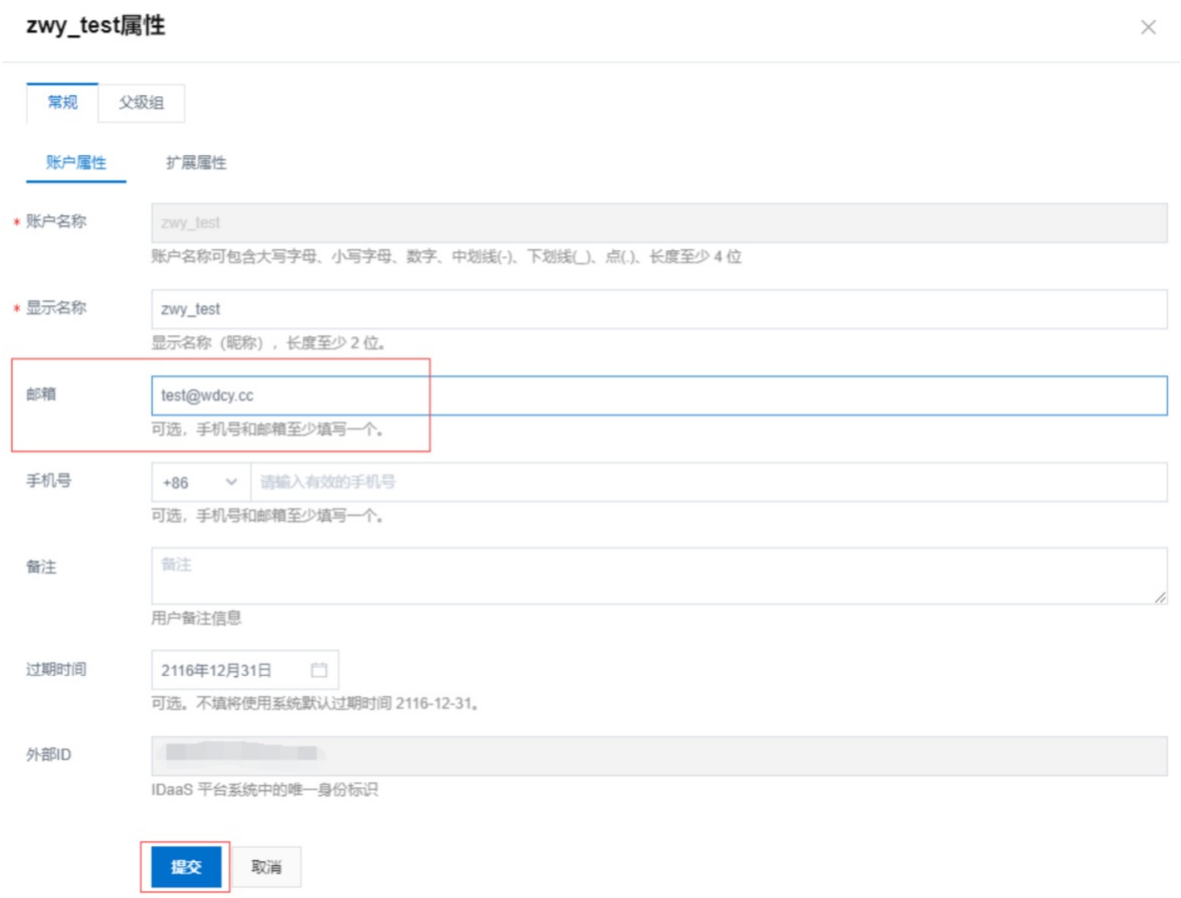


5. 给该应用配置SCIM

   组织机构和账户的同步都需要配置

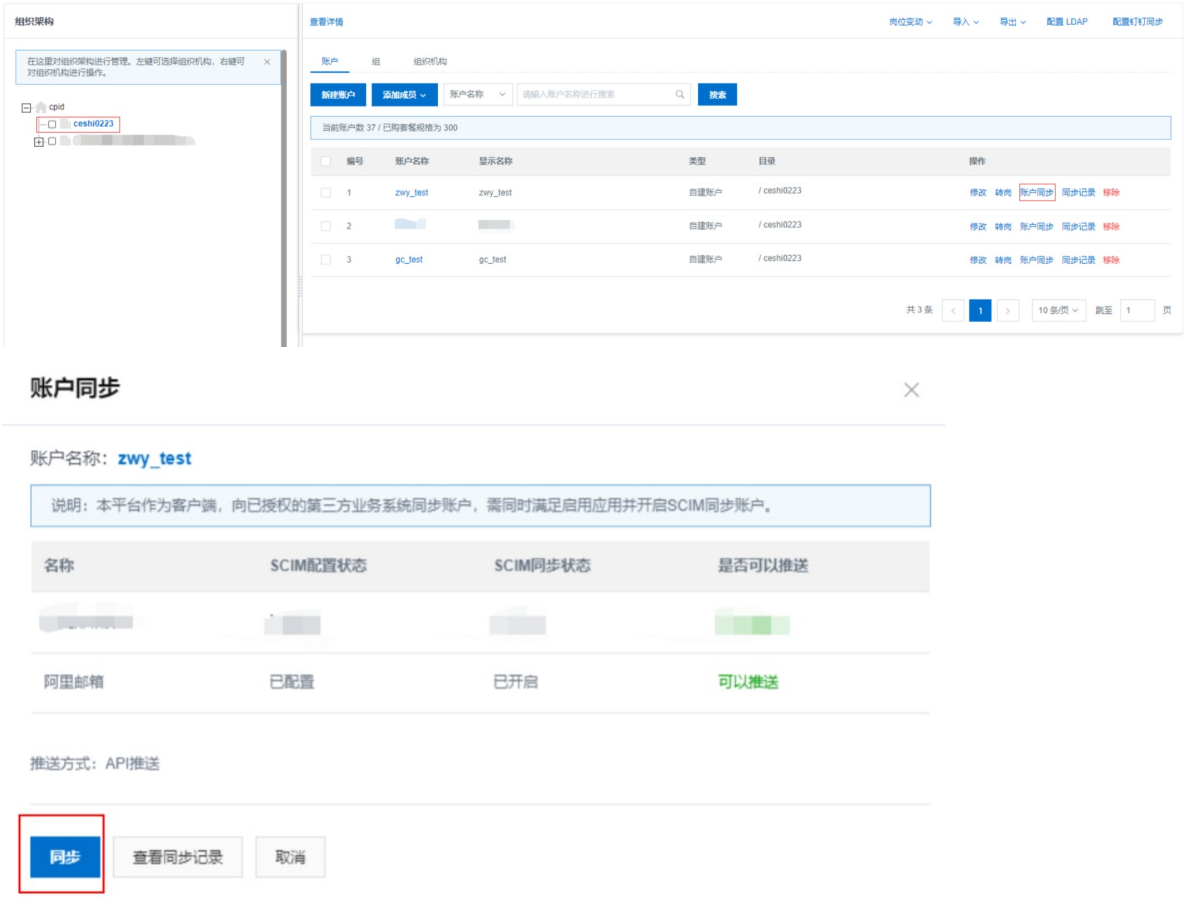
   i. SCIM同步地址使用上面步骤2在应用详情中获取的同步地址
   ii. oauth_url是IDaaS用户侧地址后加/oauth/token，见下图
   iii. client_id是应用API获取的API Key，见步骤3
   iv. client_secret是应用API获取的API Secret，见步骤3

6. 将已授权的账户邮箱格式改为阿里格式的邮箱： 想要将账户成功同步到阿里邮箱，用户申请或者管理员添加需要在IDaaS中填写该账户的邮箱，并且邮箱后缀为阿里邮箱格式，如“@wdcy.cc”。



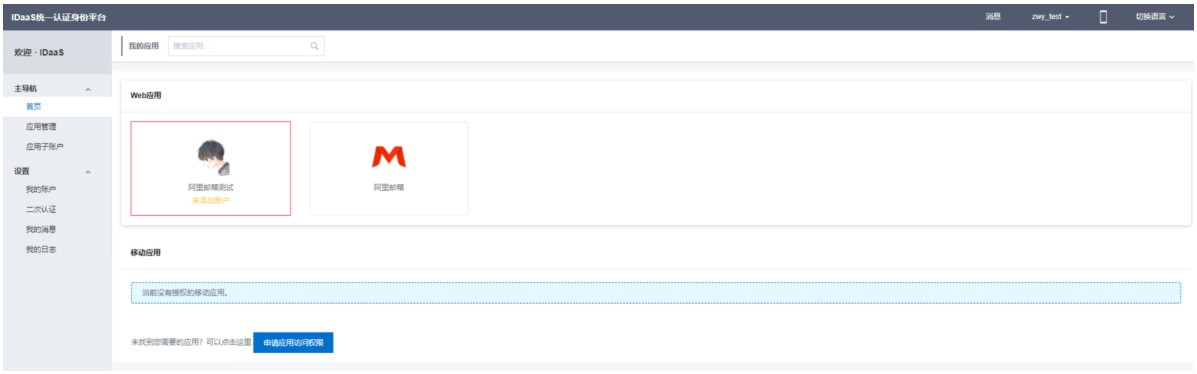
7. 同步组织机构到阿里邮箱

8. 同步账户到阿里邮箱

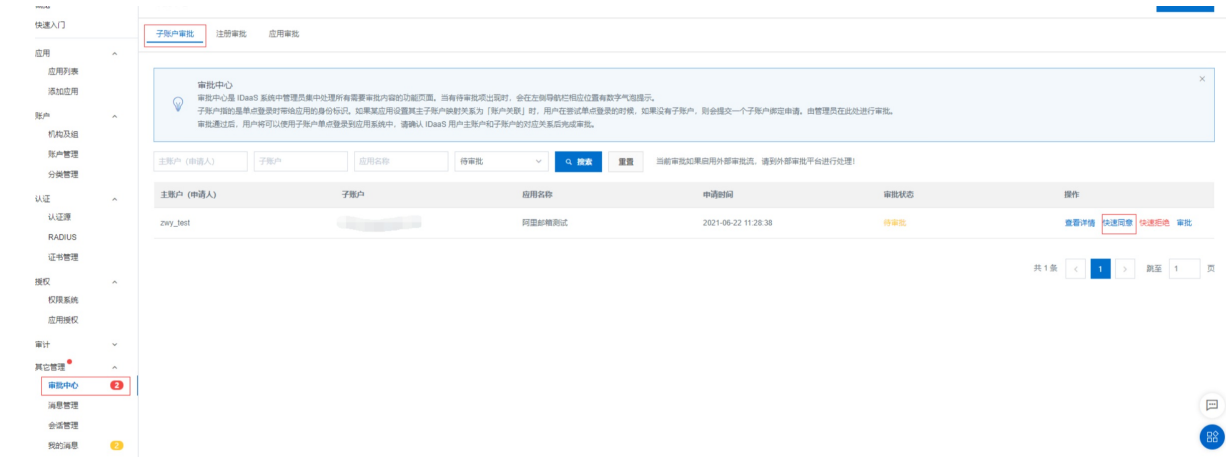


从IDaaS同步成功的组织和账户，会在阿里邮箱下图位置进行展示。

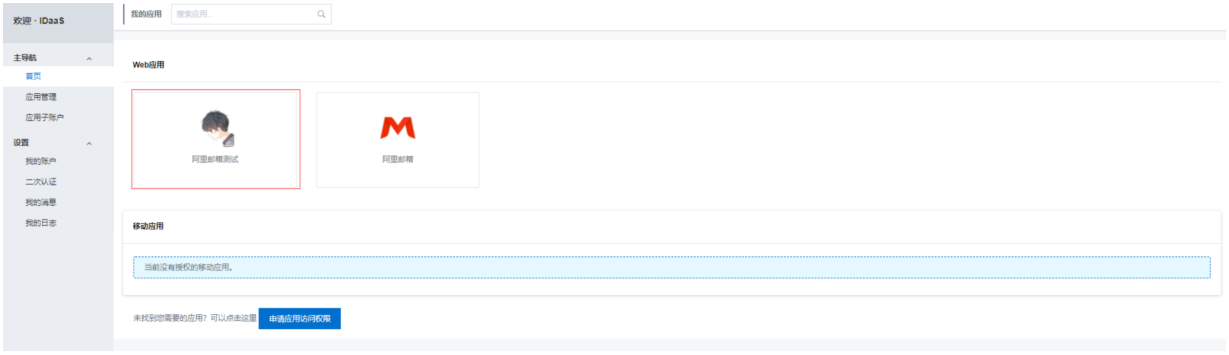
9. 用户登录IDaaS，点击阿里邮箱应用，申请将用户的邮箱添加为子账户。



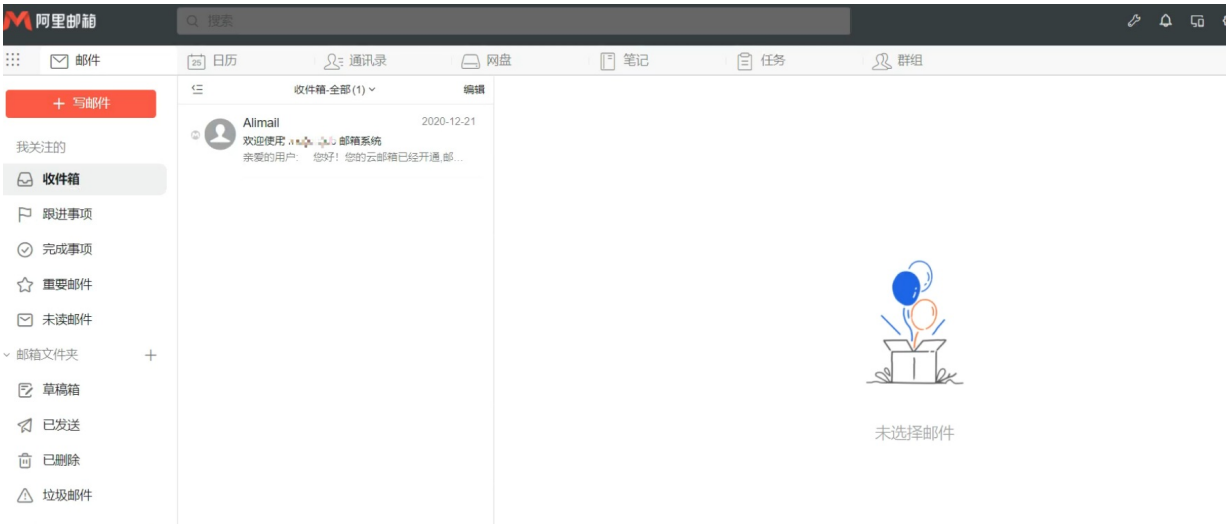
10. 管理员在审批中心下的子账户审批中对该账户添加子账户操作进行审批，并同意申请。



若以上步骤全部成功完成，用户即可在用户首页点击阿里邮箱图标进行访问。



点击上图图标，免密登录到阿里邮箱。



3.助力SSL VPN二次认证校验

背景介绍

阿里云 IDaaS 致力于统一身份认证领域，实现一个账号畅通所有应用的目的，IDaaS 与 SSL VPN 进行对接场景中，利用 IDaaS 的账户体系助力 SSL VPN 进行二次认证功能，提高 SSL VPN 登录过程的安全性。

痛点：

SSL VPN 通过证书进行身份校验，其中面临很大风险：

1. 证书可能多人使用，不需要验证使用人信息就可直接登录 SSL VPN，内部信息极容易出现泄漏风险；
2. 出现事故，无法追踪使用人员，事后无法追责；
3. 离职人员使用的证书，如果其它人也在使用，则无法及时删除离职人员的权限，出现越权行为；

IDaaS 解决方案：

IDaaS 助力 SSL VPN 认证校验，登录时除了校验用户证书，还需要输入账户和密码进行校验，实现二次认证功能。

- 如果您希望使用IDaaS的账户名和密码进行校验，可以直接在IDaaS的组织及组页面创建账户。
- 如果您希望使用AD的账户名和密码进行校验，在AD维护公司的用户信息，配置流程可以参考 LDAP认证登录。

收益：

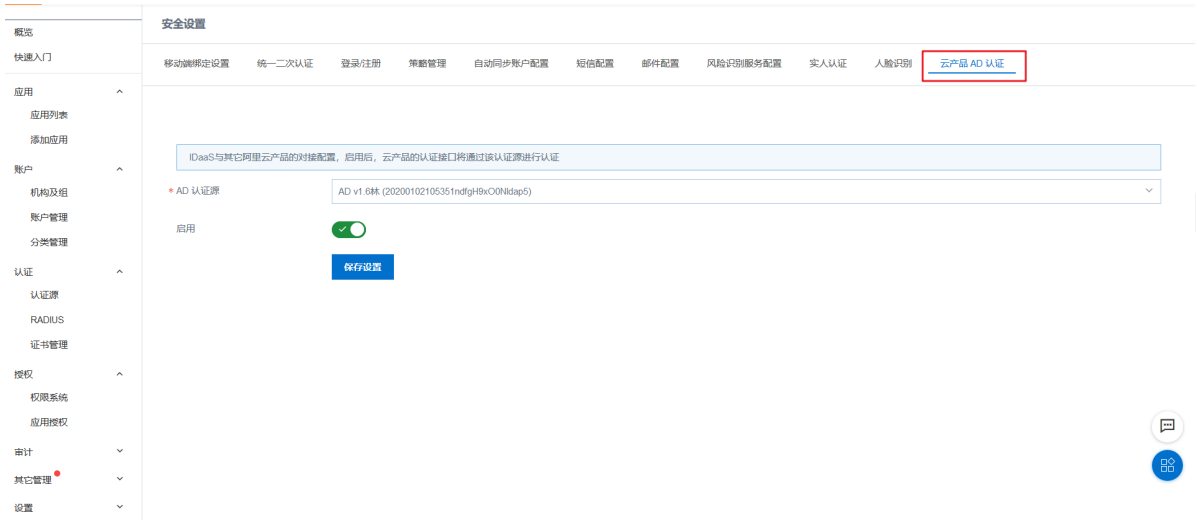
1. 一人一账户，登录信息可追踪和审计查询
2. 离职员工权限可及时收回，避免数据泄露风险

在IDaaS维护用户信息

- 参考帮助文档管理员指南-组织机构，对公司组织机构的信息进行维护。
- 参考帮助文档管理员指南-账户，对公司员工账户的生命周期进行管理。

云产品AD认证

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
2. 在左侧导航栏中点击 **认证 > 认证源** 跳转到认证源界面。
3. 创建LDAP认证源，可参考帮助文档 LDAP认证源使用手册
4. 在左侧导航栏中点击 **设置 > 安全设置** ，在安全设置页面点击 **云产品AD认证** 页签



5. 选择创建的AD认证源，启用该功能并点击保存设置。

4.阿里云应用相关FAQ

阿里云用户 SSO 配置完成后，原先RAM的登录入口就不能使用了吗

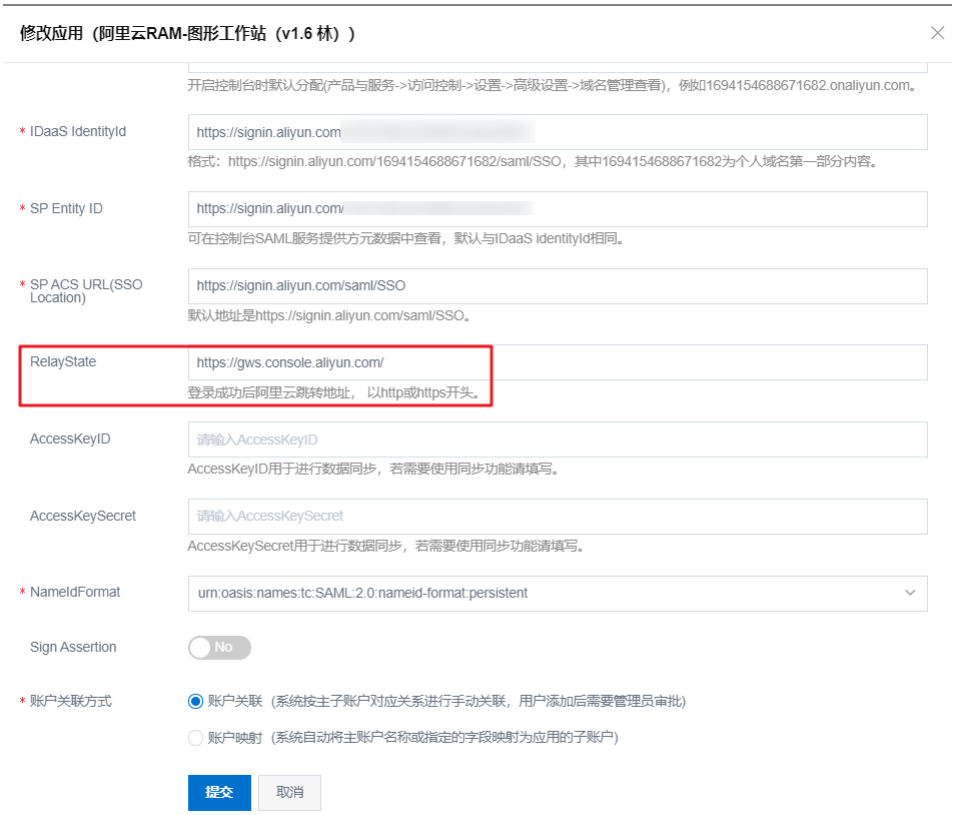
目前 RAM 开启用户SSO之后，就不能使用原先的控制台密码登录了。如果您使用的是生产的 RAM 账号，可能会影响其他人的使用。

建议您在测试的时候尽量不要使用生产的 RAM 账号 ，使用个人的 RAM 账号配置用户 SSO。

如果您需要使用生产的 RAM 账号，又不希望影响其他人的使用。您可以使用角色 SSO 作为过渡，等到正式使用 IDaaS 时再开启用户SSO 。

是否支持单点登录到其他阿里云应用，如云效、云桌面？

对于使用 RAM 账号体系的阿里云应用，是可以支持单点登录的。配置流程可以参考阿里云用户SSO。配置完成后，填写跳转地址即可。如下图：



针对用户SSO，子用户是否可以管理元数据文件？如果可以管理，子用户需要什么权限

子用户和主用户看到的SSO管理的元数据文件是同一个，如果子用户改了，则主用户看到的元数据文件也改了。子用户如果需要开启管理SSO的权限和修改元文件的权限，需要有RAM相关的全部权限(AliyunRAMFullAccess)

关于角色SSO，在IDaaS配置的“AccessKeyID”和“AccessKeySecret”的用户是否需要有RAM访问控制的权限？

需要，配置的“AccessKeyID”和“AccessKeySecret”的用户得有RAM的权限（AliyunRAMReadOnlyAccess或者AliyunRAMFullAccess），在IDAAS绑定子账户页面才可以读取到身份提供商RAM角色列表

角色SSO，在IDAAS绑定子账户页面能够选择哪些类型的角色？

能够选择的范围只能是上传了应用元文件的身份提供商对应的RAM角色，不能选择阿里云账号RAM角色和阿里云服务RAM角色