



应用身份服务 阿里云应用对接

文档版本: 20211130



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。

- 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。
- 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。
- 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。	會学者 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。	大) 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 <i>,</i> 不是 用户必须了解的内容。	⑦ 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 listinstanceid		
[] 或者 [alb]	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	05
1.1. 使用RAM用户单点登录阿里云控制台	05
1.2. 使用RAM角色单点登录阿里云控制台	14
1.3. IDaaS同步账户到RAM配置说明手册	26
1.4. IDaaS 打通 RAM 与 AD/钉钉扫码 等认证的集成	34
2.单点和同步数据到阿里邮箱	40
3.助力SSL VPN二次认证校验	50
4.阿里云应用相关FAQ	51

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。

```
[-] 阿里云 最新活动 产品、 解决方案、 云市场、 合作伙伴、 支持与服务、 开发者、 了解阿里云、
```

 訪问控制
 授欠

 全部(999+)
 网站(999+)
 帮助文哲(999+)
 开发者社区(999+)
 云市场(797)
 API错误中心(0)

 ()
 方门控制
 AM 俄您端够安全地集中管理对阿里云服务和资源的访问。您可以使用 RAM 创建和管理用户和相,并使用各种权限来允许或拒绝他们对云资源的访问。

 广品校划台
 广品文档

 用户路端
 产品快速入门
 常见问题

 原品新动态
 产品最新动态
 聚仁实践
 由户管理与分权

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

概范		10×104112 (12								
快速入门		全部 标准协	全部 标准协议 定制瞬间							
应用	^									
应用列表		22.40								
添加应用		194/Juli 本页面	WHI 配包含了所有已支持的可添加应	用列表,管理员可以选择需	要使用的应用进行初始化配置,	,并开始后续使用。				
账户	^	应用分	}为两种:一种是支持标准的 JV	WT、CAS、SAML 等模板的	应用,在这里可以通过添加对	成的标准应用模板来实现单点登录功能;另一种是定制应用,本类应用已经提供了对接其单点登录或用户同步管	9接口,由 IDaaS 为其提供定制化模糊	反进行对接。		
机构及组 账户管理		请输入应用名称				Q				
分类管理		应用圆标	应用名称	应用ID	标签	描述	应用类型	操作		
认证 认证源 RADIUS	^		腾讯企业邮	plugin_exmail2	SSO, OA, 邮件	病品企业能箱显新讯计对企业用户提供的企业都问服务。企业将自己的域名故要求进行改置后,即可则将 一般这么全域者为后端的波器和号,并可根据需要地这种号亚行自主的印刷,管理和分配。为了有物务 个全址做分子者就够不受知识它就需要的资源的干费。我们进于有限品企业都和2级市场口开发了预测路箱 (副件化)直用桌帮助客户在IDAAS中进行提集的单点登录和数据同步操作。	Web戲用	添加应用		
证书管理			\$J\$J	plugin_dingtalk	钉钉同步	们打点由阿里巴巴出品,为中国政企编身打造的免费沟通协作平台。打打同步应用是用非进行 IDaaS 与打 打之间间步的载体,实现从 IDaaS 同步数数例打招的成程。	数据同步	添加应用		
权限系统 应用授权		FORM	表单代填	plugin_aes256	SSO, AES256	表单代填可以模拟用户在登录页输入用户名和密码,再通过表单提交的一种登录方式。应用的账号密码在 IDaaS 中使用 AES266 加密解法本地加密存储。最多旧系统,不支持标准认证协议的系统成不支持改造的 系统可以使用表单代填实现统一号价管理。表单中有图片验证码,CSRF token,动态参数的场景不适用。	Web应用	添加应用		
审计	~	(-)	阿里云智能网关	aliyun_sag	Aliyun	智能錄入阅关(Smart Access Gateway)是同里云基于云原住的SD-WAN解决方案。企业可以通过智能接入阅关实现一站式输入上示,获得更加智能。更加可靠和更加安全的上云体验。	Wi-Fi设备, Web应用	添加应用		
其它管理 [●]	× ,	(-)	阿里云RAM-用户SSO	plugin_aliyun	SSO, SAML, 阿里云	基于 SAML协议,实现由 IDaaS 单点登录频用显云控制台;使用读模板,需要在RAM中为每个用户单独 创建RAM子N户,IDaaSN户和RAM子和户通过数时实现单点营录到RAM。	Web应用	添加应用		
		C-)	阿里云RAM-角色SSO	plugin_aliyun_role	SSO, SAML, Aliyun	基于 SAML协议,实现由 IDaaS 单点登录到阿里云控制台;使用该模板,需要RAM中创建RAM角色,不需要为最个用户单独创建RAM子般户,IDaaS能/F和RAM角色通过能时实现单点登录到RAM。	Web应用	添加应用		
2. 添加Sig	ningKey	y(证书)								
添加	应用	(阿里云)	RAM-用户S	SO)		×				

导入SigningKey	添加SigningKey				
别名	序列号	有效期	秘钥算法	算法长度	操作
		暂无数据			

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

添加应用(阿里云RAM-用户SSO)

* 应用名称	阿里云RAM-用户SSO
* 应用类型	─ Web应用 "Web应用"和"PC客户端"只会在用户Web使用环境中显示,"移动应用"只会在用户客户端中显 据同步"应用只用作数据的同步不会在用户侧显示,如果想在多个环境中都显示应用则勾选多
* 阿里云个人域名称	请输入阿里云个人域名 开启控制台时默认分配(产品与服务->访问控制->设置->高级设置->域名管理查看),例如 1694154688671682.onaliyun.com。
* IDaaS IdentityId	请输入IDaaS IdentityId 在 IDaaS 中设置的认证参数,它会出现在 IDaaS 导出的 metadata 里,可自定义设置。
* SP Entity ID	请输入SP Entity ID 在 SP 中设置或者生成的 Entity ID,格式统一为 https://signin.aliyun.com/1694154688671682/saml/SSO,其中1694154688671682为个人域 分内容。
* SP ACS URL(SSO Location)	请输入SP ACS URL(SSO Location) 默认地址是 https://signin.aliyun.com/saml/SSO。
RelayState	请输入RelayState 登录成功后阿里云跳转地址,以http或https开头。

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



RAM 访问控制 / 用户

用户					
RAM 用户是一个身份实体,它通常代表您的组织 通常的操作步骤如下: 创建用户,并为用户设置登录密码(用户登 2.添加用户到用户组(需要先创建用户组并完) 	R中需要访问云资源的人员或应用和 录控制台场景)或创建 AccessKey 成对用户组的授权)。	副序。 (应用程序调用 API 场	景)。		
创建用户 输入登录名、用户 ID 或 AccessKey	ID Q				
用户登录名称/显示名称	备注		弄	后登录时间 11	
p114366.onaliyun.com			-		
4. 保存应用成功,切换到应用列表,查看应用详情					
←返回					
首页 所有领域 私有云	公有云 移动 物联网	网络控制 其它			
、 应用					
应用列表			~		
添加应用 应用图标 应用名	<u>م</u>	应用ID		设备类型	
	空制台	idaas-cn-Opp 1-1, 2014	Galiytori	浏览器	
账户管理					
、 授权 应用信息	3	认证信息		账户信息 - 子OU和	1子账户
应用授权 应用的详细信息 (*	用后可编辑)	应用的单点登录地址		平台主OU/账户对/	立应用系统中子OU/账户的
(Ving系统) 查看详情		IDaaS发起地址		联表 查看应用子OU	查看应用子账户
、 以证源					
证书管理 审计信息		API			
RADIUS 查看应用系统详细的	操作日志,确保应用安全	应用对外调用的API接口			
、 审计 操作日志 查看日志 查看同	步记录	× API Key	API Secret		
导出SAML元数据文件Met adat a.xml					
② 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。

应用详情 (用户SSO)

应用图标	(-)
应用ID	n-beijing-3bo piugir
应用名称	
应用Uuld	0 24cb15374 e321e J4WQEeqHLRB
SigningKey	act)2b3aet jat 40jo6UBpjHocW
NameldFormat	um: mes:1 ameld-format:unspecified
阿里云个人域名称	11460 323 Jun.com
SP ACS URL(SSO Location)	https://si
IDaaS IdentityId	32366/sami/SSO 导出 IDaaS SAML 元配置文件
账户同步地址	in inconventione2aebd24cb1537427ab0ae321e7da66D4WQEeqHLRB
SP Entity ID	http
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

RAM访问控制	RAM访问控制 / SSO 管理
概览	SSO 管理
人员管理へ	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。
用户组	阿里云目前支持两种SSO登录方式: 1. 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。
用户	2. 通过角色 SSO,企业可以在本地 ldP 中管理员工信息,无需进行阿里云和企业 ldP 间的用户同步,企业员工将使用指定的 RAM 角色
设置	角色 SSO 用户 SSO
SSO 管理	
权限管理 へ	SSO登录设置 Z 编辑
授权	SSO 切服状态 开眉 元数据文档 已上传 ★ 下载文档
权限策略管理	SAML 服务提供商元数据 URL https://signin.aliyun.com/saml/SpMetadata.xml?tenantlD=1945
RAM角色管理	辅助域名
OAuth应用管理	
编辑 SSO 登录	设置
SSO 功能状态 🙍	
● 开启 ○ 关闭	
元数据文档 🕐	
上传文件	
辅助域名 🕜	
○ 开启	
设置域别名目通过域名	《归属校验后、SSQ 辅助域名将会失效

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

概览		应用列表					
快速入门							
应用 应用列表 添加应用	^	成 留 当	Z用列表 T理员可以在当前页面管理已经添加的所 添加完应用后,应该确认应用处于启用	所有应用,应用可以实现 单点登录和数据同步 能 时状态,并已经完成了授权。在应用详情中,可1	力。 以看到应用的详细信息、单点登录地址	L、子账户配置、同步配置、	授权、审计等信息。
账户 和构及组	^	添加应用	请输入应用名称		Q		
账户管理		应用图标	应用名称	应用ID	设备类型	应用状态	二次认证状态
分类管理		(-)	阿里云RAM-用户SSO	idaas-cn-tl326fjfx05plugin_aliyun	Web应用		
认证源 RADIUS	0					共	1条 〈 1 〉

2. 确认在IDaaS中用户是否存在,没有则创建用户

既览		机构及组		新建账户	
央速入门					
这用	^	机构及组	金砂石 账户进行管理 わ可以使用AD 11	账户属性	扩展属性 父级组
应用列表		在左側的组织架构树中,可以右键点击某个	部门对其进行操作,也可以左键选择某个部	父级	
添加应用					The sales due The
账户	~	4940 beto		* 账户名称	质尸名称
机构及组			旦信评问		账户名称不能以特殊字符开始,可包含大写字母、小写字母、数字、中划线 4位
账户管理		在这里对组织架构进行管理。左键可选 ×	账户 组 组织机构	*显示名称	显示名称
分类管理		译组织制码, 石罐可对组织制造行操作。			
人证	~		新建账户 账户名称 ~ 3	* 密码	密码
认证源		阿里云IDAAS	当前账户数 2 / 已购套餐规格为 100		只能使用大小写字母+数字+特殊字符,长度至少 10 位,密码不能包含"<"和"
RADIUS				邮箱	请输入有效的邮箱地址
证书管理			编号账户名称		手机号或邮箱至少填写一个。
受权	~		1 zbtest001	手机号	+86 ~ 请输入有效的手机号
权限系统			2 idaas_manager		手机号或邮箱至少填写一个。
成用授权				んたので	ลเช่ยเก

3. 在应用授权模块对应用进行授权

概览	应用授权	
快速入门	应用授权主体 主体授权应用	
应用 / 应用列表 添加应用 账户 /	应用 账户 组 组织机构 分类 请输入应用名称进行搜索 Q	
机构及组 账户管理 分类管理	阿里云RAM-用户SSO >>	
认证 ^		白 Dzha
RADIUS 证书管理	idaas_manager 默认管理员 ma	nag
授权 人	保存 共2条	ż.
审计 · · · · · · · · · · · · · · · · · · ·		

_

-

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

概览	应用列表			
快速入门				
应用 ^	应用列表 管理员可以在当前页面管理已经添加 当添加完应用后,应该输认应用处于	的所有应用,应用可以实现 单点登录和数据同步 能力。 。启用状态,并已经完成了授权。在应用详情中,可以看	到应用的详细信息、单点登录地址、子账户配置、同	步配置、授权、审计等信息。
账户 ^	添加应用 请输入应用名称		Q	
机构及组 账户管理	应用图标 应用名称	应用ID	设备类型 应用状态	二次认证状态 操作
分类管理	「一」 阿里云RAM-用户SSO	idaas-cn-C; DULOF _huin_uiiyun	Web应用	●× 授权 详情
认证 ^				
RADIUS	应用信息	认证信息	账户信息 - 同步	账户信息 - 子账户
证书管理	应用的详细信息	应用的单点登录地址	SCIM协议设置以及把组织机构、组	同步推送至平台主账户与应用系统中子账户的关联表
授权 ^ 权限系统	查看详情 修改应用 删除应用	IDaaS发起地址	同步机构 SCIM配置	查看应用子账户
应用授权	left len trin etc.	and 1 Minute		
审计 ~	授权信息	审计信息	API	
其它管理	应用与人员组织的授权关系	查看应用系统详细的操作日志	是否对应用开放系统API	管理应用内菜单与功能权限

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

应用列表 / 子账户

子账户						添加账户关联	批量导入
 子账户 子账户指的 举例: IDa: 账户关联方 	9是在指定应用系统中,用户: aS 中有主账户 张三(用户名 示式:在应用创建时,如果选	会以什么身份进行访问。主懸 zhangsan) ,在企业的 BPI 译了账户映射,即默认主账户	户指的是 IDaaS 中的账户。 1 应用系统中,这个用户的用 和子账户完全一致,无需配置	E进行单点登录时,IDaaS a 户名是 agoodman,即子账 置。如果选择了账户关联,则	会向应用系统传递对应的子频 户应为 agoodman,与主账F 需要在这里进行手动的子账。	⑸,该子账户需要在应用系统中存在 □ zhangsan 进行关联。 户创建和主子账户关联。	王旦可识别。
可里云RAM-用户\$	SSO						
主账户 (账户名称)			9				
账户名称	显示名称	子账户	子账户密码	是否关联	审批状态	关联时间	操作
zbtest001	zbtest001	RAM-user	无	已关联	无	2021年5月21日	删除
						共1条 < 1	> 跳至 1

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

应用身份管理	实例列表								
概览页				抓挖墙	息十田白				
EIAM 实例列表	实例ID/名称	标准版实例ID	状态 (全部) 🗸	税	数	到期时间	产品版本	用户登录贞地址	实例开放接口域名
CIAM 实例列表	idaas-cn-shenzhen]
产品文档		idaas-cn- () 📫 🗰 📭 🕅	运行中	标准版	100	2021年5月28 日	V1.8.16- GA	in aliyunidaas.com	🗈 📫 🦙 api aliyunidaas.con
101 10 101 D 1									-

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

统一身份认证	平台	
欢迎·IDaaS		我的应用
主导航	^	免登应用
应用管理 应用子账户		[-]
设置 我的账户 二次认证 我的消息	^	阿里云控制台
我的日志		仅支持移动端免暨应用 尚未获取到移动端免登应用。

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

RequestId: 61.60_1579159722125_3849 Issuer invalidated by issuer value:https://signin.aliyun.com/1949857242860803/saml/SSO

返回阿里云首页

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

使意 (Yang Angen A

3. 如何修改SSO登录后跳转的地址? 修改RelayState的值

应用ID	
	idaas-cn-zz11qd8uy05plugin_aliyun
SigningKey	14c28d882918f1a8c6dfc2e8e1a59de33SZKuwGzDCh
* 应用名称	阿里云RAM-用户SSO
* 应用类型	──Web应用 "Web应用"和"PC客户」,只会在用户Web使用环境中显示,"移动应用"只会在用户客户,」中显示,"数据同步"应用只 步不会在用户侧显示,如果想在多个环境中都显示应用则勾选多个。
* 阿里云个人域名称	请输入阿里云个人端名 开启控制台时默认分配(产品与服务->访问控制->设置->高级设置->综名管理查看),例如1694154688671682.onally
* IDaaS IdentityId	请输入IDaaS IdentityId 格式: https://signin.aliyun.com/1694154688671682/saml/SSO,其中1694154688671682为个人域名第一部分内轾
* SP Entity ID	请输入SP Entity ID 可在控制台SAML服务提供方元数据中查看,默认与IDaaS identityId相同。
* SP ACS URL(SSO Location)	游输入SP ACS URL(SSO Location) 默认地址是 https://signin.aliyun.com/saml/SSO。
* RelayState	游输入RelayState 登录成功后阿里云跳转地址,以http或https开头。

* AccossKoulD 注绘 \ AccossKoull

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

RAM 访问控制 / SSO 管理	编辑 SSO 登录设置	×
SSO 管理	SSO 功能状态 🕐	
 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。 阿里云目前支持两种 SSO 登录方式: 1. 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 2. 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。 	 开启 关闭 元数据文档 @ 上传文件 	
角色 SSO 用户 SSO	辅助域名	
SSO登录设置 ∠ 编辑		
SSO 功能状态 开启	设置域别名旦通过域名归属校验后, SSO辅助域名将	
元数据文档 已上传 上下载文档	会失效	
SAML 服务提供商元数据 URL https://signin.aliyun.com/saml/SpMetadata.xml?tenantlD=1949857242860803 辅助域名		E ?

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

	用户		
	A Sodra-Tasia, saturange-danisations, addes,		
-	An and a second an		
	1886- AMP-INDER (P-REMARK SERVery (DREARING) .		
	TABLE OF A RECEIPT AND A REAL OF ADDRESS .		
	AND AND AND A REAL OF A		
	R-2240-2140 #1	1811	81
	has sufficiently and provide	and the local division of the local division	Transaction and the
	198		and a store and
Loss	D BIZ	219478-0222-07	BARRAN BARR BA
10.018	Contract the phaneton contract of the contract		
0.488	advet .	10400000	BORNEY ROOM BO
	his style harpharatysten	219415-0210-2	BANKING BASER BM
	deput Variation of the second		
	phengdel	2944030 023	BANKAR BACK BO
	annot margin and provide state	210405233197	SURVE SUCH BY
	and a second sec		
	- 10 M	2040528032	AXION AXXA BA
	degit@degit.ordp.com	200405-05 0.028	BURRAG SUCH BR
	tells.		
NARIZM	Booker Book Booker		
NARISM	souther accel text text / №* / Southed Southers ← hzos-lcyq@zhangdh.onaliyun.com		
nalizer nit	Kosteve Recent		
алары га ~1	Konney Reset	10	3190019556
00800M FR ^SL A	Control of the second sec	u and	201020100004 201020100004
999099 111 111 111 111 111 111 111	Koney Koney Koney Koney Koney Koney Koney Koney Koney Koney Koney	00 8005 9468	analand bits. Suntananan
99809 19 19 19 19 19	term	00 98805 94466	bandari Dina Suatsanaka
	terms	uo salava artak	in management
	Image:	10 18975 1998	hang of the
	Terrery Energy Terrery Energy Terrery Energy Terrery Terre	10 1800 1904	processing processing proc
	Interventional and an an and an an and an and an	10 8000 8748	and a second
50-52M 88 94 88 88 88 88 88 88 88 88 88 88 88 88 88	term before the second se	10 1894 1.005 1.005	processo pose of part
MARCH 11日 11日 11日 11日 11日 11日 11日 11	Terrer Marine Mari	10 18800 1608 1.008	2000
		10 1894 1998 1998	anachta antiba (ant Beant 2005 -
1000204 111 112 112 112 112 112 112 112 112 11	Terrer Terrer	10 1000000	sense
1001204 22 24 25 25 25 25 25 25 25 25 25 25 25 25 25		14 1890 1603 1706	201000000 201000 201000 201000 201000 201000 201000 201000 201000 201000 201000 201000000 201000000 201000000 201000000 201000000 201000000 201000000 201000000 201000000 201000000 201000000 2010000000 2010000000 2010000000 20100000000
10.43254 20 20 20 20 20 20 20 20 20 20 20 20 20	term intervention of term	10 1800 1908 1908 1909	2000-000 2007 - 2008 -
1040204 1041 1042 1044 1044 1044 1044 10	Internet interne	20 1000 1000 1000	2000-000 2007-01 2007 2008 2008 2008 2008 2008
00.0020M		14 1944 2045 2045 2045	anaansiin anaang aa aa

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		
认证管理 加入的组	权限管理	
控制台登录管理 启用	创建AccessKey X	
控制 古 切 问 必须开启多因素认证	请及时保存或发送AK信息至对应员工, 弹窗关闭后将无法再次获取该信息, 但您可以随时创建新的AK。	
<	✓ AccessKey 创建成功	
多因素认证设备(MFA) 遵循TOTP标准算法来产生6位的 设备状态	AccessKeyID: AccessKeySecret:	
	と下载CSV文件 □ 复制	
用户AccessKey 创建新的AccessKey	确认	

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



- 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)

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。

阿里云应用对接·阿里云RAM应用对接

应用身份服务

应用身份服务

应用ID	wanglialiyun_role2	
SigningKey	5795412077857392270(CN=dr)	
* 应用名称	阿里云RAM 角色 SSO926	
* 应用类型	✔ Web应用	
* IDaaS IdentityId	IDaaS	
	IDaaS平台身份标识,如:IDaaS	
* SP Entity ID		
	服务薅标识,固定值,如:um:alibaba:cloudcomputing	
 SP ACS URL(SSO Location) 	「 / で 30 昭在地路 mm //rights aligns com/com/ relation	
	INCOSINI-PATURONE, PERZEN, P., Indo-Fragmin, any Unit. Companing Ordersou	
* NameldFormat	persistent V	
* SP登录方式	应用自定义登录页 ~	
RelayState	请输入RelayState	
	登灵成功后阿里云跳转地址,以http或https开头	
AccessKeyID		
	用于查询RAM角色列表,推荐使用RAM子用户AccessKeyID	
AccessKeySecret		
	出了更调KAM用出列表,推导成HKAM于H广AccessReySectel	
Sign Assertion	No	
* 账户关联方式	●账户关联-RAM角色(系统按主子账户对应关系进行手动关联,用户选择添加后需要管理员审批)	
	提交 取消	
保存应用成功,切换	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)	

[-] 阿里云RAM 角色 SSO926	wanglialiyun_role2	Web应用		授权 详情 🔺
应用信息	认证信息	账户信息 - 子账户	同步	授权信息
<u>或用約许細結卷(</u> 情用后可銅鑽) 查看评情	应用的单点 登录 地址 IDaaS发起地址	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		应用与人员组织的授权关系 授权
审计信息	ΑΡΙ			
查看应用系统详细的操作日志 查看日志 查看同步记录	应用对外调用的APH接口			

应用图标	[-]
应用ID	wanglialiyun_role2
应用名称	阿里云RAM 角色 SSO926
SigningKey	5795412077857392270(CN=dr)
NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
SP ACS URL	https://signin.aliyun.com/saml-role/sso
IDaaS IdentityId	IDaaS 导出 IDP SAML 元配置文件
SP Entity ID	urn:alibaba:cloudcomputing
RelayState	
AccessKeyID	LTAI4FgWZSznz6gJemaVWD2e

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

Ð	管理控制台					搜索	Q	消息	费用	工单	备案	:
	产品与服务 >										×	(
	云服务器 ECS	Q、 靖输入关键词						_				
¥	云数据库 RDS 版	最近访问										
8	专有网络 VPC	访问控制	*	应用身份服务					弹性计算			
~	对象存储 OSS								数据库			
	VIRT-III 033	弹性计算		数据库		存储与CDN			存储与CD	N		
×	CDN	云服务器 ECS	*	云数据库 POLARDB		对象存储 OSS	*		网络			
Å	负载均衡	负载均衡	*	云数据库 RDS 版	*	文件存储 NAS			分析			
₽	域名	弹性伸缩		云数据库 MongoDB 版		表格存储			云通信			
		容器服务		云数据库 Redis 版		归档存储			监控与管理	里		
3	云市场	容器服务 Kubernetes 版		云数据库 Memcache 版		CDN	*		应用服务			
	数加控制台概览	容器镜像服务		云数据库 HybridDB for MySQL		PCDN			互联网中间	可件		
		资源编排		云数据库 HBase 版		全站加速			消息队列	MQ		
		批量计算		时序时空数据库 TSDB		云存储网关			移动云			
		函数计算		分析型数据库 PostgreSQL版		智能云相册			视频服务			
		弹性高性能计算		云数据库 OceanBase		混合云备份			大数据 (∛	绞力口)		
		轻量应用服务器		分析型数据库		混合云容灾			安全 (云)	盾)		
		图形工作站		数据传输服务 DTS		安全加速 SCDN			域名与网站	占 (万网)		
		确性容器实例 FCI		数据管理 DMS		怨的复体管理						

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。

RAM访问控制	RAM访问控制 / SSO 管理			
概览	SSO 管理			
人员管理 へ	阿里云支持基于 SAML 2.0 的 SSO (Single Sign O	n,单点登录) , 也称为身份联合登录。		×
用户组	阿里云目前支持两种SSO登录方式: 1. 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。		
用户	2. 通过角色 SSO,企业可以在本地 IdP 中管理员]	「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。	
设置	角色 SSO 用户 SSO			
SSO 管理 权限管理	在企业IdP方配置时,请使用如下阿里云SAML服务 https://signin.aliyun.com/saml-role/sp-metadata.	提供商元数据URL: ml 🕘 复制		
授权	< 新建身份提供商			c
权限策略管理	身份提供商名称 备注	创建时间	更新时间	操作
RAM角色管理	ceshi926	2019年9月26日 14:52:45	2019年9月26日 14	:52:45 删除
OAuth应用管理	1112	2019年8月6日 14:48:58	2019年8月6日 14:4	48:58 删除
	eccec	2019年8月5日 23:55:16	2019年8月5日 23:	55:16 删除
	XXXX	2019年8月5日 23:54:40	2019年8月5日 23:	54:40 删除
RAM访问控制	RAM访问控制 / SSO 管理		新建身份提供商	×
概赏	SSO 管理		 提供商名款 	
人员管理へ		单点登录),也称为身份联合登录。	DELO/160 P4101	
用户组	阿里云目前支持两种SSO登录方式: 1. 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。	最多包含128个字符,允许英文字母、数字、	特殊字符, 不能以特殊字符开头或结尾。
用户	2. 通过用色 550, 企业可以在本地 10P 中管理负工作		amiteria Ko 备注	
设置	角色 SSO 用户 SSO		最大长度256个字符	
SSO 管理	在企业IdP方配置时,请使用如下阿里云SAML服务损 https://signin.alivun.com/saml-role/so-metadata.xm	供商元数据URL:	* 元数据文档	
NRETE A		. 🖬 ocini	上传文件	
2000年時時間	新建身份提供商		由身份提供商生成的元数据文档	
RAM角色管理	身份提供商名称 备注	创建时间		
		2019年9月26日 14:52:45		
OAuth应用管理				
OAuth应用管理		2019年8月6日 14:48:58		

- 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。

RAM访问控制	RAM访问控制 / SSO 管理			新建身份提供商	
概览	SSO 管理				
人员管理 用户组 用户	阿里云支持基于 SAML 2.0 (阿里云目前支持两种SSO登 1. 通过用户 SSO,企业员工 2. 通过角色 SSO,企业可以	G SSO (Single Sign On,单点登录) ,也 录方式: 在登录后,将以 RAM 用户身份访问阿里z 在本地 IdP 中管理员工信息,无服进行问		身份提供商创建成功	
设置	角色 SSO 用户 SSO			为确保身份提供商的正常使用,请为身份提供商新 前往新建RAM角色	健RAM角色
SSO 管理 权限管理	在企业IdP方配置时,请使用 https://signin.aliyun.com/sa	如下阿里云SAML服务提供商元数据URL: iml-role/sp-metadata.xml (] 复制			
授权	新建身份提供商				
权限策略管理	身份提供商名称	督注	创建时间		
RAM角色管理	ceshi926		2019年9月26日 14:52:45		
OAuth应用管理			2019年8月6日 14:48:58		
			2019年8月5日 23:55:16		

阿里云应用对接·阿里云RAM应用对接

新建RAM角色			>
→ 选择类型	2	配置角色 3 创建完成	
选择可信实体类型 身份提供商			
* 角色名称			
不超过64个字符,允许英	文字母、数字,或"-"		
备注			
最大长度1024字字符			
* 选择身份提供商			
ceshi927			~
限制条件			
条件关键词	限定词	值	

 上ー步
 死の
 米団

 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"。

 新建RAM角色
 ×

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

 ●
 ●
 ●

✔ 角色创建成功!					
为确保角色的正常使用,建议您继续为此角色添加权限					
	为角色授权	精确授权			

添加权限							
被授权主体 test927@role.zhangdh.onaliyuns	被授权主体 test927@role.zhangdh.onaliyunservice.com X						
选择权限							
系统权限策略 > 请输入	×	Q	已选择(1) 清晰	ŧ			
权限策略名称	备注	^	AliyunRAMReadOnlyAccess X				
AdministratorAccess	管理所有阿里云资源的权限						
AliyunOSSFullAccess	管理对象存储服务(OSS)权限						
AliyunOSSReadOnlyAccess	只读访问对象存储服务(OSS)的权限						
AliyunECSFullAccess	管理云服务器服务(ECS)的权限						
AliyunECSReadOnlyAccess	只读访问云服务器服务(ECS)的权限						
AliyunRDSFullAccess	管理云数据库服务(RDS)的权限						
AliyunRDSReadOnlyAccess	只读访问云数据库服务(RDS)的权限						
AliyunSLBFullAccess	管理负载均衡服务(SLB)的权限						
AliyunSLBReadOnlyAccess	只读访问负载均衡服务(SLB)的权限						
AliyunRAMFullAccess	管理访问控制(RAM)的权限,即管理用户以及授权的权限						
AliyunRAMReadOnlyAccess	只读访问访问控制(RAM)的权限,即查看用户、组以及授税 在自Ath和限	2					

确定取消

- 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。

应用图标	四用应 动名称 这		设备类型	应用状态		操作	
J	DefaultAppfortest2 k94b4f24cfb193f558fb39aa213c1b70TIXXhUP k99		麲	牧据同步		授权	详情 ▼
C - J	阿里云RAM 角色 SSO926	wanglialiyun_role2	wanglialiyun_role2 Web应用			授权	详情 ▲
应用信息	ž	认证信息		账户信息 - 子账户	同步	授权信息	
应用的详	并细信息 (禁用后可编辑)	应用的单点登录地址		平台主账户与应用系统中子账户的关联表		应用与人员组织的授权关系	
查看详情	5	IDaaS发起地址 7		查看应用子账户		授权	
审计信息	1	API					
查看应用系统详细的操作日志		应用对外调用的API接口					
查看日志 查看同步记录		API Key API Secret					

应用身份服务

					:	添加账户关联			\times
Ð	如用列表 / 子账户								
	∊子账户				•	* 主账户(邮箱/手机号/ 账户名称)	主账户(邮箱/手机号/账户名称)		
						* 账户关联-RAM角色	请选择	^	1
	阿里云RAM 角色 St	SO926					Aliyun-Role-All Aliyun-Role-Read		Ī
					۹		ceshi926		
	账户名称	子账户	显示名称	子账户密码	是否关联		Role-all Role-read		
	wang925	role-read	wang925	无	已关联		test927		
	wangli	role-all	wangli817	无	已关联				
	wangli	ceshi926	wangli817	无	已关联				
RAMID	16)tžalu s	RAM的问控制 / RAM的色管理							
概范	1	RAM角色管理							
人団管理 用户(用) 役置 SSO 管理 収用管理		什么是RAM角色? RAM向色1時間時間ではないたは(物気: RAM やご言称で下からAMI用・(可能量になー) ・等に気がいつからAMI用・(可能量になー) ・そに気かしたなの期間ができい(電影支払) ・通知目前日前後、(電影支払) ・通知目前日前後、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきも、(電影支払) ・たいからきます。(電影支払) ・たいからます。(電影支払) ・たいからます。(電影) ・たいからます。(電影) ・たいからます。(電影) ・たいからます。(電影) ・たいからうます。(電影) ・たいからきます。(電影) ・たいからうる) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからうます。(電影) ・たいからう ・たいのう ・たいからう ・たいのう ・たいからう ・たいのう ・たいの ・たいのう ・たいのう ・たいの ・たいの ・たいの ・たいの ・たいの ・たいの ・たいの ・たいの	用户、某个应用或用重去服务) (特許助40%后端服务) (因激访问) 20%行报件) 月還作了補證供服务) 使凭成为一种要变金的授予访问 显示一组的原来),如果認識要任	出日照我的一种完全方法,根据不同应用结果 双期的方法。 把服料书式面色的功能,请参考6446万限标	,受伤任的云体可能有如下 <u>!</u> 略(Policy)。	些例子:			×
校開創	策略管理	新建RAM角色 输入角色名称或新注	Q						
RAM#18	色管理	RAM角色名称		備注			创建时间	操作	
OAuth应	の用管理	Aliyun-Role-All		拥有访问控制权限			2019年5月10日 20:02:43	添加权限 精确授权 删除	
		Aliyun-Role-Read		访问控制只读权限			2019年5月10日 20:03:45	添加权限 精确接权 删除	
		ceshi926					2019年9月26日 14:53:15	派加权限 精确授权 删除	
		Role-all		拥有访问控制的编辑	双環		2019年5月10日 14:22:50	添加权限 精确接权 删除	
		Role-read		拥有访问控制的只读机	反視		2019年5月10日 14:21:50	添加权限 精确授权 删除	
		test927					2019年9月27日 17:31:58	添加权限 精确接权 删除	
		添加权限							

五、从IDaaS单点登录到阿里云控制台

1. 开启应用

2.

概览	1	应用列表					添加应用
快速入门	^	请输入应用名称		٩			
应用列表		应用图标	应用名称	应用ID	设备类型	应用状态	操作
添加应用 账户	^	J	DefaultAppfortest2	854b4f24cfb193f558fb39aa213c1b70TIXXhIJP hd9	数据同步		授权 详情 ▼
机构及组 账户管理		C -J	阿里云RAM 角色 SSO926	wanglialiyun_role2	Web应用		授权 详情 ▼
分类管理	~	FORM	表单代填	wangliaes2561	Web应用		授权 详情 ▼
认证源 RADIUS		Cus	CAS(标准)-31	wanglicas_apereo3	Web应用		授权 详情 ▼
证书管理		-	SAP GUI	wanglics_sap_gui1	PC客户讲	×	授权 详情 ▼
105.407	~						

3. 在IDaaS中创建一个用户

应用身份服务

概览	机构及组				数据字典
快速入门					
应用 ^	组织架构	王丽的公司 查看详情			岗位变动 ~ 导入 ~ 导出 ~ 配置 LDAP
应用列表	- 王丽的公司	■ 账户 组 组织	机构		
漆加处用			- 100 - 40		
账户 ^	++ C === 860ali	11911人名称进行	1908	<u> </u>	
账户管理	🗆 🔜 ceshi823	编号 账户名称	显示名称	类型 目录	操作
分类管理	- C hellobug1	1 test919	test919	自建账户 / ceshi88 /	修改 转岗 账户同步 同步记录 离职
认证 ^	- C 🛄 ou831				
认证源	C 0 -	2 zzd66	zzd66	新建一个IDaaS用户	修改转岗账户同步同步记录离职
RADIUS	- C in ou8314	3 test924	test924	自建账户 /	修改转岗 账户同步 同步记录 离职
证书管理	C	4 wang925	wang925	白澤咲户 /	修改 转动 联合同步 同步记录 窗町
			Mangozo	Left Block	
5. 在应用授权模块对应)	用进行授权				
6. 概览	应用授权				
快速入门	按应用授权组织机构档	按组织机构/组授权应用	用 按账户授权应用	用 按应用授权账户 分	分类授权应用
应用	^				
应用列表		在这里使用不同方式为应用进	行授权分配。		
账户	IDaaS 支持	多种多样的授权方式: 可以选	定一个应用后,为其划;	定授权到的组织机构/组的范围;	也可以选定—个账户,并为其分配有权限访
机构及组					
	应用 (1)		组织机	构和组(1426) 已授权(1404)个
账户管理					
分类管理	阿里云RAM 角色 SS	60926	m :	代表组织机构, 😹 : 代表组。	
认证 认证源	へ 阿里云RAM 角色 S	SO926	 请输入 	组名进行搜索	
DADIUO				王丽的公司	
RADIUS		共1条 〈 1 〉		→ 狼群	
证书管理				◎ ● 委托认证测试	
+===+=7				- ♀ ■ 测试同步的组织机构	
反权				asdasdsadas	
应用授权				R ntv34	
权限系统				asd	
分级管理				R izvt	
				. R D Managed Service Accou	ints
审计	~		-	Real Program Data	
其他答理	~			. R D ForeignSecurityPrincipa	Is
				C III System	
7. 访问普通用户登录地	址,copy下面的链接				
8. ? 说明					
请到云盾IDaaS控制	台页面查看下面链接				
实例列表					云命令行(Cloud Shell) 🗙
实例ID/名称	状态 (全部) 🗸 – 規	格授权 创建时间	到期时间 用戶	⊐访问的Portal的sso地址	用户访问的Portal的api地址
idaas-	运行中 基	础版 2019年5月6日	2019年8月7日 ce	gin.aliyunidaas.com)i.aliyunidaas.com
					·
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		

欢迎·IDaaS	我的应用
主导航 ^	Web©IE
首页	The second se
应用管理	
应用子账户	
设置 ^	
二次认证	
我的消息	
#245 D +	
找的口志	移动应用
	当前没有授权的移动应用。

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

应用列表	风峰点登录和数据同步能力。 发权。在应用详情中,可以看到应用的详细信息、单	图标	C-J
踌辕入应用名称		应用ID	idaas-cn-zz11qd8uy05plugin_aliyun_role
应用图标 应用名称	应用ID	应用名称	阿里云RAM-角色SSO
「」 阿里云RAM-角色SSO	idaas-cn-zz11qd8uy05plugin_aliyun_role	SigningKey	2e900298870a72b038843ac7ce43f0cdxt5dA8xeh38
应用信息	认证信息	SP Entity ID	um:alibaba:cloudcomputing
应用的详细信息	应用的单点登录地址	IDaaS IdentityId	21312 导出 IDaaS SAML 元配置文件
查看详情修改应用删除应用	IDaaS发起地址	NameIdFormat	urn oasis names to SAML 2.0 nameid-format persistent
授权信息	审计信息	SessionDurationTim e	1 3600 RAM支持的会话时长
应用与人员组织的授权关系	查看应用系统详细的操作日志	Binding	POST
授权	查看日志 查看同步记录	SP ACS URL(SSO Location)	https://signin.aliyun.com/saml-role/sso
		Sign Assertion	无

如何修改SSO登录后跳转的地址?



			-
	修改应用(阿里云RAM	I-角色SSO)	\times
	* 应用名称	阿里云RAM·角色SSO	
	* 应用类型	✔ Web应用 "Web应用"和PC客户满"只会在用户Web使用环境中显示。	
<u>言息、单点登录地址、子</u> !	* IDP IdentityId		
	* SP Entity ID	IDaS子台身份标记, 単品登录时用于正規IDaaS, 可自定义, 知IDaaS, urr.alibaba:doudcomputing 総合場時日、周完値、如: urr.alibaba:doudcomputing.	
yun_role	* NameldFormat	urn: oasis:names:tc:SAML-2.0:nameid-format:persistent	
	* Binding	POST ~	
	* 会话时长	默认POST方式发送消息到阿里云控制台。 1小时 ~	
	* SP ACS URL(SSO	RAM支持的会活时长 https://signin.aliyun.com/sami-role/sso	
	Location)	2020 Data Chata	1
	relayolate	IggmL/Lotainy Guine 登录成功后阿里云跳转地址,以http或https开头。	

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。

	Requestid: 96.227_1595498527124_5014 Issuer invalidated by issuer value:12321 逐回阿里云首页
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	
一)阿里云 错误提示	
	Requestid: 96.2章 ^章 , 智多的 000多基于 (Hitler Hitz Can't find the intended audience in at least one AudienceRestriction 近回阿里云首页
报错提示:提示时间不匹配	

阿里云应用对接·阿里云RAM应用对接



The min of duration seconds is 900, the max of duration seconds is 3600, but your value is 10800. RequestId: 98.91_19 = 5/-

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。

概览		← Aliyun CSI	JefagitRole
人员管理	^		
用户组		基本信息	
用户		RAM 角色名称	AliyunCSDefaultRole
设置		备注 最大会话时间	容器服务(CS)在集群操作时默认使用此角色来访问您在其他云产品中的资源 3600 秒 编辑
SSO 管理			
权限管理	~	权限管理 信任策略	管理
授权		添加权限 精确授权	
权限策略管理		权限应用范围	权限策略名称
RAM 角色管理		全局	Aliyun.

OAuth 应用管理 (公测中)

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,正因拢着越来
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

-)	管理控制台					搜索	Q	消息	费用	工单	备案	í
	产品与服务 >										×	(
	云服务器 ECS	Q、 请输入关键词						_				
Ŧ	云数据库 RDS 版	最近访问										
8	专有网络 VPC	访问控制	*	应用身份服务					弹性计算			
~	对象存储 055	/							数据库			
	ATTREE A	弹性计算		数据库		存储与CDN			存储与CDN	V		
×	CDN	云服务器 ECS	*	云数据库 POLARDB		对象存储 OSS	*		网络			
A	负载均衡	负载均衡	*	云数据库 RDS 版	*	文件存储 NAS			分析			
₽	域名	弹性伸缩		云数据库 MongoDB 版		表格存储			云通信			
		容器服务		云数据库 Redis 版		归档存储			监控与管理	E		
35	云市场	容器服务 Kubernetes 版		云数据库 Memcache 版		CDN	*		应用服务			
₽	数加控制台概览	容器镜像服务		云数据库 HybridDB for MySQL		PCDN			互联网中间	引件		
		资源编排		云数据库 HBase 版		全站加速			消息队列 N	ЛQ		
		批量计算		时序时空数据库 TSDB		云存储网关			移动云			
		函数计算		分析型数据库 PostgreSQL版		智能云相册			视频服务			
		弹性高性能计算		云数据库 OceanBase		混合云备份			大数据 (数	女力口)		
		轻量应用服务器		分析型数据库		混合云容灾			安全 (云盾	旨)		
		图形工作站		数据传输服务 DTS		安全加速 SCDN			域名与网边	よ (万図)		
		通性変異なるよう		※は知味田 DMS		知識情体等理				. (

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。

=	(一) 阿里云
---	---------

☰ (-) 阿里云		Q 搜索文档、控制台、API、解决方室和资	調用 工单	普索 🖄	业 支持	官网 🔄	۵.	₩ @
RAM访问控制	RAM访问控制 / 用户							
概范	用户							
人员管理 ^	● RAM 用户是一个身份实体,它通常代表您的组织中需要询问云资源的人员或应用程序。							
用户组	遷常的操作步骤如下:							
用户	1. 创建用户,并为用户设置量景密码(用户量景控制结场器)或创建 AccessKey(应用程序调用 API 场裂)。 2. 淡如用户到明户组(需要先创建用户组并完成对用户组的进权)。							
设置 	総論用 ^{AA} 総入型景名、用户 ID 惑 AccessKey ID, Q							
SSO 管理 初期管理 へ	用户整要名称/显示名称 衛注	013B	间		操作			
授权	Lest03@189406305540386.onaliyun.com test003	2020	₽5月14日 15:31:45		添加到用。	中组 添加权用	#8%	

4. 点击账户名称进入账户详情页面,点击创建AccessKey

RAM访问控制 / 用户 / test003@1894063505540386.onaliyun.com

← test003@1894063505540386.onaliyun.com

	用户基本信息	编辑基本信息	
	用户名	test003@1894063505540386.onali 🚨 复制	UID
	显示名称	test003	创建时间
	备注		手机号码
	邮箱	test003@a.com	
	认证管理	加入的组 权限管理	
	控制台登录管理	■	
	您的账号已开启用	月户SSO,因此控制台登录配置不生效,所有RAM用户将使用SSO登录控制台。	
	控制台访问	未开启	上次登录控制台时
<	必须开启多因素认		下次登录重置密码
	夕田吉 :117:04		
	多 因素从证收f	育 (MIFA) 同用虚拟MFA设备	
	遵循TOTP标准算》	去来产生6位数字验证码的应用程序	
	设备状态	未启用	
	用户 AccessKe	у	
ſ			
l	BIXE ACCESSIO	2) TOUSH	

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

			○ 搜索文	档 控制台 API 解决方案和资源
			- BESICK	
RAM访问控制 / 用户 / test003@1894063505540386.onaliyun.com				
← test003@189406350554038	6.onaliyun.com			
				
用戶基本信息 编辑基本信息				
用户名 test003@1894063505540386.onali	复制		UID	224792789441
亚示名称 test003			HINEHTIDI	2020年5月14日
⊯/工 邮箱 test003@a.com	DIJÆ ACCESSNEY			×
	 请及时保存或发送 Access 	Key 信息至对应员工,弹窗	关闭后将无法再次获取该	§信息,但您可以随
认证管理 加入的组 权限管理	的创建新的 AccessKey。			
	🕑 创建成功,请及时保存	•		
控制台登录管理。 启用控制台登录				
您的账号已开启用户SSO,因此控制台登录配置不生效,所有RAM用F	AccessKey ID	LTAI4G		
控制台访问 未开启	AccessKey Secret	xKahLv		
必须开启多因素认证				
	丛下载CSV文件 ☐ 复制			
				关闭
				2013
新用户设置管理RAM的权限(AliyunRAMFullAccess)				
奂到权限管理标签,点击添加权限				
RAM访问控制 / 用户 / test003@1894063505540386.onaliyun.com				
(to at 0.0.2 @ 1.80.40(.2.5.0.5.5.40.2.8)				
Clest003@1894063505540366.	onaliyun.com			
用户基本信息 编辑基本信息				
用户名 test003@1894063505540386.onali 🔾 复想	a)		UID	224792789441505364
显示名称 test003 1、点击权	限管理		创建时间	2020年5月14日 15:31:45
备 注			手机号码	
邮箱 test003@a.com				
¥				
认证管理 加入的组 权限管理				
个人权限 继承用户组的权限				
7847/IHOCPR				
权限应用范围 权限策略名称	权限策略类型	督注		
		1	令有数据	

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。

. 2、点击添加权限

添加权限							×	
* 被授权主体								
test003@	1894063505	540386.onaliyun.com	×					
* 选择权限								
◉ 系统策略		三义策略 新建校	仅限策略			已选择 (1)	清除	
RAM					G			
权限策略名利	\$	备注				AliyunkamFullAccess X		
AliyunRAMF	ullAccess	管理访问	可控制 (RAM) 的权限,即	管理用户以及授权的	权限			
AliyunRAMR	eadOnlyAcc	:ess 只读访问	可访问控制 (RAM) 的权限 5权限	,即查看用户、组以	及授			
		\backslash	\mathbf{X}					
			、 直接点击即可选	择				
							(L)	
							E?	
点	击确定道	进行保存						
							R	
确定	取消							
aaS添加阿里	里云控制	台						
[用列表 中选打	译阿里云	RAM-用户SSO添	加应用					
戦速	添加应用							
用 ^	<u>全部</u>	标准协议 定制模板						
应用列表 添加应用	G	添加应用 本页面包含了所有已支结的可还如	100用列表,管理员可以从中洗掘杀望神田	的应用进行初始化配霉,并开始后	续使用.			
iin ^	v	应用分为两种:一种是支持标准的	h JWT、CAS、SAML 等機板的应用,在這	(里可以通过添加对应的标准应用制	更被来实现单d	國豪功能:另一种是定制应用,本类应用已经提供了对接其单点强亲助	就用户同步的接口,由 IDaaS 为其提供定制	时化横板进行对接。
机构及组 账户管理	请输入应用	用名称				Q.		
分类管理	应用图标	应用名称	标签 描述		woring-m -		nce teststille with the second	応用美型
	FORM	表单代道	家单代 SSO, AES256 获单代 认证物	項可以積积用戶任登录贝編入用户 议的系统或不支持改造的系统可以		MELUNEPHERX的一种量浆方式。此用的账号密码在 IDaaS 中使用 AES2 运输统一身份管理。泰单中有图片验证码、CSRF token、动态参数的5	200 加密赛波本地加密存储,很多旧系统。 杨晨不通用。	小文時标准 Web应用
RADIUS 证书管理	E STET	4J4J	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	由阿里巴巴出品,为中国政企量。 步拉取到IDaaS和时时增量变更触	时造的免费沟 設同步到IDaa	通协作平台。钉钉同步应用是用来进行 IDaaS 与钉钉之间双向同步的复 IS。	就体,IDaaS 实现了由 IDaaS 增量同步到	时时,从时时 数据同步

基于 SAML 协议,可以实现由 IDaaS 单点雅灵到阿里云控制台,使用阿里云控制台的子账户进行访问。

基于 SAML 协议,可以实现由 IDaaS 单点登录到阿里云控制台,使用阿里云控制台的 RAM 角色进行访问。

SSO,用户同步,SAML, 基于 SAML 协议,实现由 iDasS 到阿里邮箱的单点登录和用户同步。

2. 添加SigningKey(证书)

权限系统 应用授权

分级管理 审计 •

C-)

C-)

M

阿里云RAM-用户SSO SSO, SAML, 阿里云

阿里云RAM-角色SSO SSO, SAML, 阿里云

阿里邮稿

操作

添加应用

添加应用

添加应用

添加应用

漆加应用

Web应用

Web应用

Web应用

阿里云应用对接·阿里云RAM应用对接

应用身份服务

统一身份认证平台				添加应用 (阿里云	添加SigningKey		×
概定				E) Signing Key			
快速入门				43/Calgininghey	* 名称	调输入名称	
应用 ^				362	部门名称	-832E102人的Hit	
应用列表				CN=test1, ST=sc, C=CN	公司名称	调输入公司各称	
深肌应用			,并开始后续倒 1应的标准应用概	CN=alyun-muzi, ST=北守 C=CN	* 国家	調选择	~
机构及组				CN=alyun-muzi, ST=北部 C=CN	* 筆价		
账户管理							
分类管理			描述		城市	调输入域市	
	6-1		基于 SAML t		*证书长度	論选择	~
RADIUS			STI-OAM J. SIG.		* 有效期	请选择	~
证书管理	(-)		基于 SAML 整 要为每个用户			提交 取消	
援权 ^	M		基于 SAML t				
权限系统							
版用授权							
UEBA ^							

- 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, identityld和SP identityld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 Identityld: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 获明	双方式如下:				
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			
 管理控制台 	× ← 账号管理 × +				- 🗆 ×
\leftarrow \rightarrow C \textcircled{m} acco	unt.console.aliyun.com/#/secure				☆ 🙂 :
		Q 搜索文档、控制台、API、解决方案和资源	费用 工单 备案 企业	支持 官网 🖸	Ţ. Ä 🕲 👳 🔞
账号管理	安全设置				
安全设置	登録新号: klaas test (原己通过整名以近)				
基本资料	账号ID: 10973:				点击右上角用户头像
实名认证	注册时间: 2019年2月15日下午5:34:00				
地址管理	修改头像				
学生认证					

- ◎ 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
- NameldFormat: 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

←选择signingKey		×
* 应用名称	阿里云RAM-用户SSO 111	
* 应用类型	☑ Web应用 "Web应用"和"PC客户端"只会在用户Web使用环境中显示,"移动应用"只会在用户客户端中显示,"数据同步"应用只用作数据的同步不会在用户侧显示, 如果想在多个环境中都显示应用则勾选多个。	
*阿里云个人域名称	1757331455.onaliyun.com 开启控制台时默认分配(产品与服务->访问控制->设置->高级设置->域名管理查看),例如1694154688671682.onaliyun.com	
* IDaaS IdentityId	https://signin.aliyun.com/17575(31455/saml/SSO 格式: https://signin.aliyun.com/1694154688671682/saml/SSO,其中1694154688671682为个人域名第一部分。若在公测版设置中关闭了租户特有经销商选项可以为任意值。	i
* SP Entity ID	https://signin.aliyun.com/1757)1455/saml/SSO 可在控制台SAML服务提供方元数据中查看,默认与IDaaS identityId相同	
* SP ACS URL(SSO Location)	https://signin.aliyun.com/samWSSO 默认地址昰nttps://signin.aliyun.com/sam//SSO	
RelayState	調驗入RelayState 聲景成功后阿里云說转地址,以http感https开头。	
AccessKeyID	LTAI4Fbd6qA7Vc)Va AccessKeyID用于进行数据同步,若需要使用同步功能请填写。	
AccessKeySecret	wUtivMr1rCnwHKdk	
* NameldFormat	um:oasis:names:tc:SAML:1.1:nameid-format:unspecified ~	
* Binding	Post ~	
* SP登录方式	应用自定义登录页 ~	
Sign Assertion	No	
*账户关联方式	 ● 账户关联(系统按主子账户对应关系进行手动关联,用户添加后需要管理员审批) ○ 账户映射(系统自动将主账户名称或指定的字段映射为应用的子账户) 	



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。

構造	应用列表						添加应用
快速入门							
应用	请输入应用名称			٩			
应用列表	应用图标	应用名称	应用ID	ite	备类型	应用状态	操作
源加应用	6.7	回用于RAM.用白SSO	wathiskan26	100	wh在目		运行 举运 ,
账户	C)	Partition (1) 000	incestituity and o		ew/22/13		150. Frig =
机构及组							
账户管理	应用信息		认证信息		账户信息 - 子账户	同步	授权信息
分类管理	应用的详细信	1息(狭用后可编辑)	应用的单点登录地址		平台主账户与应用系统中子账户的关联表		应用与人员组织的授权关系
认证 ~			ID == 942274044		来表向中工彩山		9847
认证源	a a integr		NAME OF COLUMN AND ADDREED ADD		PERMITENCE 2 MAY 1		2004
RADIUS							
证书管理	审计信息		API				
授权 个	查看应用系统	钱详细的操作日志。	应用对外调用的API接口				
权限系统	***	*****		171 0			
应用授权		Eenprux	APIKey	API Secret			
分级管理							

应用详情 (阿里云RAM-用户\$SO 111)

应用图标	C-J
应用ID	yanshialiyun4
应用名称	阿里云RAM-甩户SSO 111
SigningKey	8291927404164392560(CN=aliyun02)
NameldFormat	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
阿里云个人域名 称	1757 .onaliyun.com
SP ACS URL	https://signin.aliyun.com/saml/SSO
IDaaS IdentityId	https://signin.aliyun.com/175 155/saml/SSO 导出 IDaaS SAML 元时置文件
账户同步地址	/api/application/aliyun/account/b5b5a6 35056c03rKz1PbS5TTd
SP Entity ID	https://signin.aliyun.com/175 //saml/SSO
SP Entity ID Binding	https://signin.aliyun.com/175 \$/saml/SSO POST
SP Entity ID Binding Sign Assertion	https://signin.aliyun.com/17? POST 已禁用
SP Entity ID Binding Sign Assertion RelayState	https://signin.aliyun.com/175 š/saml/SSO POST 已禁用
SP Entity ID Binding Sign Assertion RelayState AccessKeyID	https://signin.aliyun.com/175 POST 已禁用 LTAI4Fbd6qA7
SP Entity ID Binding Sign Assertion RelayState AccessKeyID AccessKeySecret	https://signin.aliyun.com/175 3/saml/SSO POST 已禁用 LTAI4Fbd6qA72Va wUtivMr1rCnwt2an5X2
SP Entity ID Binding Sign Assertion RelayState AccessKeyID AccessKeySecret 应用状态	https://signin.aliyun.com/175 3/saml/SSO POST 已歸用 LTAI4Fbd6qA7 JVa wUtiwMr1rCnwt Can5X2 启用
SP Entity ID Binding Sign Assertion RelayState AccessKeyID AccessKeySecret 应用状态 账户关联方式	https://signin.aliyun.com/175 s/saml/SSO POST 已禁用 LTAI4Fbd6qA7 dVa wUtivMr1rCnwF Can5X2 启用 账户关联
SP Entity ID Binding Sign Assertion RelayState AccessKeyID AccessKeySecret 应用状态 账户关联方式 创建人	https://signin.aliyun.com/175 s/saml/SSO POST 已歸用 LTAI4Fbd6qA7 JVa wUtiwMr1rCnwł Can5X2 启用 账户关联

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。

1	联进		应用列表						添加应用
ł	H速入门								
8	如用	^	请输入应用名称				Q		
	应用列表		应用图标 应用名称		应用ID		设备类型	应用状	恣 操作
,	添加应用 50户	^				wceshialiyun_role9	Web应用	~) 授权 洋橋 ◄
2. 依	次选择 详	₹选择 详情 > 同步							
1	应用图标	应用名称			应用ID		设备类型		操作
	「可里云RAM-用户SSO 111		yanshialiyun4		Web应用		授权 详情 🔺		
	应用信息			认证伉血			账户信息 - 子账户	同步	接段信息
	应用的详细信	總 (禁用后	(可编辑)		应用的单点登录地址		平台主账户与应用系统中子账户的关联表		应用与人员组织的授权关系
	<u> </u>		IDaaS发起地址		查看应用子账户		授权		
			API						
	查看应用系统	も洋細的操作			是否对应用开放系统API	101.0			
	宣君曰志	重管问题	PICR		API Key	AM Secret			

3. 点击**SCIM配置**链接,进入配置页面:

SCIM 配置 (阿	列里云RAM-用户SSO 111))	<
账户	组织机构				
应用名称	阿里云RAM-用户SSO 111				
* SCIM同步地 址	https://yanshi. ######## ############################	api/application/aliyun/accour com/api/application/scim/acc	nt/b5b5a6bc30e433 count	3rKz1PbS5TTc	
是否开启	开 の	账户时会向已经授权的应用	推送账户		
协议类型	○ Basic ● OAuth2 应用提供的保护接口的协议类型				
* oauth url	https://yaidp4.idsmanager.com/o	auth/token			
* client_id	c100c49c031760e9f8	jWPtkkjC9			
* client_secret	xryepHyUCRY2Q2Sb client_secret 必填	DE9ud5akpm			
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	容去掉	
是否开启:开 协议类型:选 oauth url:当 client_id和clie	启此开关 择OAuth2 前IDaaS域名地址+/oauth/token ent_secret:第二部分第5步获取的API	Key和API Secret			
⑦ 说明	IDaaS域名地址可以在 <mark>云盾IDaaS管理</mark> 控	制台获取。			
实例列表					云命令行(Cloud Shell) 🗙
实例ID/名称	状态 (全部) ∨	规格授权 创建时间	到期时间	用户访问的Portal的sso地址	用户访问的Portal的api地址
idaas-	运行中	基础版 2019年5月6日	2019年8月7日	ce, gin.aliyunidaas.com	bi. aliyunidaas.com
					く上一页 1
在IDaaS中创建	建一个用户				
概流	机构及组				政府字典
快速入门 应用 ^ 应用列表	● 料地及通 管理用在三輪页面対相応等称。即1及其包含的组、能户进行管理、 在左側的相称称称中,可以為提供由某个部门对其进行操作,也可	也可以使用AD、LDAP或Excel文件的方式配置导入或同 以左键选择某个部门,并在右侧均其进行创建所户、创	步。 動組、创建即门等操作,		×
源加应用	组织架构	朝阳区 查看洋情			岗位变动 > 导入 > 导出 > 配置 LDAP
机构及组 账户管理	在这里对组织架构进行管理。左键可选择组织机构,右键可对组织 × 机构进行操作。	新中 組 組织が物 新建築户 英加成英 - 新輸入名称进行	按案	۹	
77,488-48 认证 ^		当前账户数为 15,许可证额账为 100000			
认证源 RADIUS	⊕ 0 <u></u> . 1 #	编号 账户名称	显示名称	类型 目录和描述	操作
证书管理 授权 ^		2 lisi001	acc1 IIsi001	目編明中 /北京/朝阳区/	都改 转商 财产同步 同步记录 都設 修改 转向 账户同步 同步记录 都設

5. 在**应用授权**模块对新应用进行授权

4.

阿里云应用对接·阿里云RAM应用对接

概览	应用授权
快速入门	按应用接权组织机构组 按组织机构组接权应用 按账户接权应用 按应用接权账户 按分类接权应用
应用 ^ 应用列表 添加应用 账户 ^	按账户授权应用 直接为指定账户授权指定应用。 提示:这里展示的并不是「账号是否有某应用权限」,而是「账号是否直接授权到某应用」。账号同样可以通过其所属组织机构、所属组等渠道获取某应用的权限。可以通过账户管理查看到某个账户所拥有的所有应用权限信息。
机构及组	账户(1) 应用数 (10) 已授权(0)个
账户管理	Lenard Michael Michael
分类管理	IISI001
认证 个	lisi001 → 应用名称
认证源	□ 阿里云RAM-用户SSO 111
RADIUS	×1 家 く ■ 2 阿里元RAM-用户SSO 110
证书管理	
授权 个	回 阿里云RAM-用户SSO-03
权限系统	回 阿里云RAM-角色SSO-03
应用授权	回
分级管理	

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

概范												
快速入门												
应用 ^ 应用列表	机构及组 管理员在当前页面对组织架构。部门及其包含的组、账户进行管理 在左侧的组织架构制中,可以右键点击其个部门对其进行操作。也可以可以用于一个部门对其进行操作。也可以可能。	也可以使用AD,LDAP或Excel文件的方式配置 可以左續连择某个部门,并在右侧为其进行创建则	导入或同步。 4户、创建组、创建部门等操作。			×						
添加应用	组织媒构	朝阳区 查看详情	總知区 监影计信									
账户 ^	在这里对组织原构进行管理。左腱可选择组织机构,右键可对组织 ×	1 10 10 10 10 10 10 10 10 10 10 10 10 10										
账户管理	10.約進行操作。		名称进行搜索	Q.								
分类管理		二前所由計力 16 法市民運動市力 1000	00									
认证 ^ 认证源		编号 账户名称	显示名称	安臣	目录和描述	操作						
RADIUS		□ 1 acc1	acc1	自建账户	/北京/朝阳区/	停改转为 账户同步 同步记录 移脉						
证书管理 1547 0		2 lisi001	lisi001	自建烁户	/北京/朝阳区/	停改 转声 账户同步 同步记录 移除						
权限系统												
应用援权												
账户同步				×								
账户名称: lis	i001											
说明:本平	台作为客户端,向已授权的第三方业务系统同步账	户, 需同时满足启用应用并开放	自SCIM同步账户。									
名称	SCIM配置状态	SCIM同步状态	是否可以推送									
阿里云RAM·	用户SSO 111 已配置	已开启	可以推送									
戸歩 选择 同步 按钮 点击同 步记录 7. 阿里云控制台 切换到阿里云	营育同步记录 取消 1完成同步。 受查看同步结果: 中查看同步过来的账户 - 控制台中: 人员管理 > 用户菜单,人	员列表中可查看到新向	步过来的账户:									
RAM访问控制	RAM访问控制 / 用户											
概范	用户											
人员管理	へ RAM用户是一个身份实体,它通常代表您的组	設中需要访问云资源的人员或应用程序。										
用户组	通常的操作步骤如下:											
用户	 1.创建用户,并为用户设置登录密码(用户登 2.添加用户到用户组(需要先创建用户组并完 	景控制台场景)或创建AccessKey (应用程 成对用户组的授权) 。	李调用API场景)。									
设置	新建用户 用户登录名称 >> 清縮	Q										
SSO 管理	用户登录名称/显示名称		香注	创建时间		操作						
权限管理 授权	lis:001@1757566569331455.onaliyun	.com		2020年1月7日 23:00:22		添加到用户组 添加权限 删除						
	121001											

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:

- 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

◎ 阿里云IDAAS.认证云IDaaS平台 × +		- 🗆 X
← → C ▲ 不安全 dexuavjsho.login.aliyunidaas.com/login?_auth=202001021	05351ndfgH9xO0NIdap5&re_sp_login=true	☆ ⊖ ⊙
	同日本 DAAS	
	当前登录力式为AD认证源	
	邮箱/手机号/账户名称 [
	2009	
	清 输入验证弱	
	気管	
	第三方账户登录	

操作步骤

- 以Ⅱ管理员账号登录云盾IDaaS管理平台。具体操作请参考 Ⅲ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。

应用	^	ド 表単代填 (v1.6 林)	202001021	Web应用	~ 0	授权 详情 ▼
应用列表添加应用		[] 阿里云RAM·角色SSO (v1.6 林)	202001021	Web应用		授权 详情 ▼
账户 机构及组 账:白额理	^	[-] 阿里云RAM-用户SSO(v1.6 林)	20200102	Web应用		授权 详情 🔺
分类管理		应用信息	认证信息	账户信息 - 子账户	同步	授权信息
认证 认证源	^	应用的详细信息 (禁用后可编辑)	应用的单点登录地址	平台主账户与应用系统中子账户的关联表		应用与人员组织的授权关系
RADIUS 证书管理		查看)羊筒	IDaaS发起地址	查看应用子账户		授权
授权 权限系统	^	审计信息	API			
应用授权		查看应用系统详细的操作日志	是否对应用开放系统API			
审计 其它管理 ●	~		API Key API Secret			F
设置	~					

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

阿里云应用对接·阿里云RAM应用对接

应用身份服务

应用	^	FORM	表单代填 (v1.6 林)	202001021	Web应用	\checkmark	授权	详情 ▼
应用列表添加应用		כ	阿里云RAM-角色SSO (v1.6 林)	20200102	Web应用		授权	详情 ▼
账户 机构及组	^	C -J	阿里云RAM-用户SSO(v1.6 林)	2020010;	Web应用		授权	详情 🔺
账户管理								
分类管理		应用信息		认证信息	账户信息 - 子账户	同步	授权信息	
认证 认证源	^	应用的详细信	题 (禁用后可编辑)	应用的单点登录地址	平台主账户与应用系统	中子账户的关联表	应用与人员组织的授权关系	
RADIUS		查看详情		IDaaS发起地址	查看应用子账户		授权	
证书管理								
授权	^	审计信息		API				
应用授权		查看应用系统	详细的操作日志	是否对应用开放系统API				
审计	~	查看日志	查看同步记录	API Key API Secret				
其它管理	~							

	M	
阿里云 [DAAS	
当前登录方式为 AD认证加	<u>a</u>	
邮箱/手机号/账户名称		
密码		
请输入验证码	/MNU 2-	
登录	ŧ	
第三方账		
CO LDAP LDAP	AD认证源	

⑦ 说明 您也可以在设	置 > 安?	全设置 > 登录/注	主册页签下,i	配置SF	P发起	己登录认证	正方式。右	在访问IDaas	S发起地	址时即	叩可以(使用指	定的认	人证方言	式进行	5认证登	^姜 录。				
								Q 搜索3	文档、控制台	合、 API、 角	解决方案和	口资源	费用	工单	备案	企业	支持	官网	۶.,	۵.	Ä
概 <u>员</u> 快速入门		安全设置																			
应用	^	移动端绑定设置	统一二次认证	登录/)	主册	策略管理	短信配置	n 邮件配置	风险识	别服务配	置 3	实人认证									
应用列表添加应用																					
账户	^	注册			和	用户登录相关(的一些配置。														
机构及组账户管理		登录			账户制	婝															
分类管理								开启后用户在	登录失败时	将被限制的	失败次数。										
认证	^				IDaaS	3发起登录认证	E方式	账户+密码()	默认) 10338分表	× ≈⊐≪440		- តាបត	10000000110001	* 白家双武	©≂+nt##	4818728 15 4	60.00.00.00	二方外部	1.7781-0-1	可经别样	-701
RADIUS				ſ				方认证页面。	1044020	E.aCoco 404.		47 · J 6046		40 64950	400-000-010	200302007	AH-1-AE353				
证书管理				l	SP发	起登录认证方式	式	AD认证源 ・								T接跳					
授权	^							转到三方认证	贞面。												
应用授权								保存设置													
审计	~																				
其它管理	~																				
设置	^																				
个性化设置 安全设置																					
	_																				

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。

应用	^	表单代填 (v1.6 林)	202001021	Web应用		授权 详情 ▼	
应用列表 添加应用		[] 阿里云RAM-角色SSO (v1.6 林)	202001021	Web应用		授权 详情 👻	
账户 机构及组	^	[] 阿里云RAM·用户SSO(v1.6 林)	20200102	Web应用		授权 详情 🔺	
账户管理							
分类管理		应用信息	认证信息	账户信息 - 子账户	同步	授权信息	
认证	^	应用的详细信息 (禁用后可编辑)	应用的单点登录地址	平台主账户与应用系统中子账户的	1关联表	应用与人员组织的授权关系	
认证源							
RADIUS		查看详情	IDaaS发起地址	查看应用子账户		授权	
证书管理							
授权	^	审计信息	API				
权限紧统							
应用授权		查看应用系统详细的操作日志	是否对应用开放系统API				
审计	~	查看日志 查看同步记录	API Key API Secret				P
其它管理	~						по
设置	~						

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

? 说明

h

您可以在设置 > 安全设置 > 登录/注册页签下,配置SP发起登录认证方式。在访问IDaaS发起地址时即可以使用指定的认证方式进行认证登录。

	可里云			Q 搜索文档、控制	則台、API、解決方案和资源 费用]	単 备案	企业 支持 官	∞ ⊡ <u>¢</u> ' 1
账户	^	安全设置						
が/AJX3日 账户管理		移动端绑定设置统一二次认证 登录	(注册 策略管理 短信配置	邮件配置				
分类管理								
认证	î î							
认证源		注册	和用户登录相关的一些配置。					
RADIUS		登录	账户纷纷					
业书管理			NIV TRAE		时将被限制失败次数。			
授权	^							
权限系统			Daas友起登录认证力式	账户+密码(默认) 选择用户访问IDaaS发	▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶	密码或添加其他	认证源,如果是第三方	外部认证则会直接跳转到三
应用授权				方认证页面。				
审计	×		SP发起登录认证方式	钉钉扫码登录_林	~			
其它管理	^			选择用户访问SP(应用)	系统)发起登录系统的认证方式,可以配置默认	的账户密码或漆	加其他认证源,如果是	第三方外部认证则会直接跳
审批中心	4			+9351_73 #A4L94000				
同步中心				保存设置				
消息管理 会汗禁頭								
安約海南								
3400 3173/24								
设置	^							
中午後期								
ATMA								
应用	^	表单代填 (v1.6 林)	202001021		Web应用			授权 详情 ▼
添加应用		[-] 阿里云RAM-角色SSO (v1.6 #	t) 20200102		Web应用			授权 详情 ▼
账户 机构及组	^	[-] 阿里云RAM-用户SSO(v1.6 林	20200102		Web应用			授权 详情 ▲
账户管理								
分类管理		应用信息	认证信息		账户信息 - 子账户	同步	授权信息	
认证	^	应用的详细信息 (禁用后可编辑)	应用的单点登录地址		平台主账户与应用系统中子账户的关联表	1	应用与人员组织的授	权关系
认证源		香香洋梅	IDaaS (公共)		香香应用乙醛白		把切	
KADIUS		2010 F 1 1 1	100001012/04L				100	
近ち直理		441144-05						
授权	^	审计信息	API					
1×1R系統 応用授权		查看应用系统详细的操作日志	是否对应用开放系统API					
		查看日志 查看同步记录	API Kev	API Secret				
жи ••••••••••••	Ť							

	阿里云IDAAS-预发环境	
\square	邮箱/手机号/账户名称	
	密码 请输入验证码	
	忘记密码? 登录 【打扫冊登录林 しAP () () () () () () () () () () () () ()	

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

😑 (-) 阿里記	E	a Ite					Q 搜索	義用 工单 备实	企业 支持 App E	0 W C	简体 🌔
概況		添加应用									
快速入门		全部 标准协会	义 定制模板								
应用	^										
添加应用 🖌	- 1	添加5 	如用 把含了所有已支持的可添加感	7用列表,管理员可以选择需要	· 使用的应用进行初始化配置	并开始后续使用。					×
账户	^	应用分	为两种:一种是支持标准的 J	WT、CAS、SAML 師模板的E	应用,在这里可以通过添加对	应的标准应用模板来实现单点整要功能;另一种是定制应用,本类应用已经	提供了对接其单点登录或用户同步的接口,由!	DaaS 为其提供定制化模板	进行对接。		
机构及组账户管理		请输入应用名称				- Q -					
分类管理		应用图标	应用名称	应用ID	标签	描述			应用类型	操作	
认证 认证源	^	M	腾讯企业邮	plugin_exmail2	SSO, OA, 前1年	關訊企业邮總量將訊針对企业用户還供的企业邮局服务。企业将自己的域 根据需要对这些帐号进行自主的组织。管理和分配,为了帮助各个企业能 本接口开发了關訊邮稿(插件化)应用未有助整户在IDAAS中进行便證的	洺按要求进行配置后,即可拥有一批以企业域 对于邮箱账号及组织架构更方便的进行管理, 单点登录和数据同步操作。	名为后缀的邮箱帐号,并可 我们基于嚮讯企业邮箱V2版	Web应用	添加应	₩
RADIUS 证书管理			4747	plugin_dingtalk	4141同步	fff最由阿里巴巴出品,为中国政企最身打造的免费沟通协作平台。ffff 数据9ffff的流程。	周步应用最用来进行 IDaaS 与钉钉之间同步的	载体,实现从 IDaaS 同步	数据同步	添加应	Ħ
接权 权限系统	^	F	表单代這	plugin_aes256	SSO, AES256	愚单代脑可以翻刻用户在登录页输入用户各印密码,再通过患举描支的一 密存储,很多旧系统、不支持标准认证协议的系统或不支持改造的系统可 token、动态参数的场景不适用。	种登录方式。应用的账号签码在 IDaaS 中使用 以使用衷单代编实现统一身份管理。表单中有I	l AES256 加密算法本地加 图片验证码、CSRF	Web应用	添加应	用
应用授权 审计	÷	כ־כ	阿里云智能网关	aliyun_sag	Aliyun	智能接入网关(Smart Access Gateway)是阿里云基于云原生的SD-WAP 智能、更加可靠和更加安全的上云体验。	W解决方案。企业可以通过智能接入网关实现一	站式接入上云,获得更加	Wi-Fi设备, Web应用	源加应	19
其它管理	č	כ	阿里云RAM-用户SSO	plugin_aliyun	SSO, SAML, 阿里云	基于 SAML 协议,实现由 IDaaS 单点登录到阿里云控制台;使用该模板, 户遗过映射实现单点整录到RAM。	需要在RAM中为每个用户单独创建RAM子账	中,IDaaS账户和RAM子账	Web应用	添加应	用
10 M		כ	阿里云RAM-角色SSO	plugin_aliyun_role	SSO, SAML, Aliyun	基于 SAML 协议,实现由 IDaaS 单点登录到阿里云控制台;使用该模板, IDaaS账户和RAM角色通过原射实现单点登录到RAM。	需要RAM中创建RAM角色,不需要为每个用。	中单独创建RAM子账户,	Web应用	添加应	
		M	阿里邮箱	plugin_alimail	SSO, 用户同步, SAML, 阿里云, 邮箱	基于 SAML 协议,实现由 IDaaS 到阿里邮箱的单点登录和用户同步,			2 Web应用	》 添加应	•
		W	WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress 是全世界最初广泛使用的 CMS(Content Management Syste 面,允许千万技术或非技术人员生产、管理各种类型的网站。从商业网站 IDaaS 支持通过 SAML 协议单点登录到 WordPress 网站。	em,內容管理系统),它通过非常强大的操件; i、政府页面到个人嫁餐、主题论坛,WordPre:	系统和方便目然的操作界 18 所支持的形式非常多样。	Web应用	添加应	ŧ

 \times

添加应用 (阿里邮箱)

图标	 ・上传文件 田片大小不超过1MB
应用ID	idaas-cn-beijing-3bohwti7ffkplugin_alimail2
* 应用名称	阿里邮箱
* 应用类型	✔ Web应用 "Web应用"只会在用户Web使用环境中显示。
* AppCode	請输入AppCode AppCode由阿里邮箱提供,用于单点登录
* AppSecret	请输入AppSecret 由阿里开发商提供,用于单点登录。
AccessCode	请输入AccessCode 由阿里开发商提供,若需要同步人员组织则需要填此项。
AccessPassword	请输入AccessPassword 由阿里开发商提供,若需要同步人员组织则需要填此项。
* AccessTarget	请输入AccessTarget 目标域名,如:mxhichina.com;若需要同步人员组织则需要填此项。
* 邮箱登录地址	请输入邮箱登录地址 登录阿里企业邮箱的地址,如:https://mail.mxhichina.com
本系统根OU的外部ID	请输入本系统根OU的外部D 本系统中假组织机构的外部d,系统中"机构及组->根组织机构的详情"中可查看。
*账户关联方式	 账户关联(系统按主子账户对应关系进行手动关联,用户添加后需要管理员审批) 账户映射(系统自动将主账户名称或指定的字段映射为应用的子账户)
	提交 取消

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。

o p 🛛 post	master				查看		
收件人:	oungstreng.gunds						
✓ 发送成功	撤回邮件						
发送邮件超	过30天,已无法获取详细发送状态。	,					
	±						
WS接口甲证	育, SS0 中 请						
	+	*	-	2	••••		
公司即相或名	名: <u>nttp://</u>						
公司名称:							
申请测试环境	竟域名: http://theit.eg.cc						
目前测试环境	竟的出口 ip:	1					
需要访问的排	妾口:账户及组织架构同步						
单点登录:	需要 appCode, appSecret						
访问接口:	雲要 accessToken _ acces	Target					
"本系统根OU外部id"为ID	aaS的rootOU的外部id 管理员可以在账户及组中。	5击rootOU的"	杳看详情" 中	获取。			
应用 ^	机构及组			<i>x</i> - <i>v</i> (0			
应用列表	管理员在当前页面对组织架构、部门及其包含的组、 在左侧的组织架构树中,可以右键点击某个部门对打	账户进行管理,也可 基于操作,也可以达]以使用AD、LDA E键选择某个部门。	P 或 Excel文件的 并在右侧为其进	方式配置导入或同步。 行创建账户、创建组、创	建部门等操作。	
添加应用							
账户 ^	组织架构	3	着 洋情				
账户管理	在这里对组织架构进行管理。左键可选择组织机构,右键可	J ×	账户 组	组织机构	1		
分类管理	对组织机构进行操作。		9098K-0	※白夕☆ し	法检入账户复杂进行编制	E (3-40t
认证 ^	E cpid		WIGEXIO ⁻¹	44 .20 ×	HEAL CAPA CAPACITY ISS		14284
认证源 RADIUS	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		当前账户数 37 /	已购套餐规格为:	300		
江北等理			编号	账户名称	显示名称		

证书管理

 \times

cpid属性

组织机构属性	_
* 名称	cpid
	请编入组织或部门名称。
外部ID	A COPIER OPERATE C
	若编入外部ID,则必须唯一,若有值不可做惨改。
描述	描述
	说明部门的功能,特点等。
组织UUID	shee rookes rookultu jirook eering seren ud hillood
	组织的UUID,唯一,调用API时UUID是必要条件。

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。

应用详情	(阿里邮箱)
------	--------

图标	M
应用ID	idaas-on-b eeling- Jeeneer his to pl_ass of
应用名称	阿里邮箱
应用Uuid	50x8102300000000000000000000000000000000000
AppCode	
AppSecret	
AccessCode	
AccessPassword	
AccessTarget	
邮箱登录地址	
组织机构同步地址	
账户同步地址	
邮箱RootOu的ID	
本系统根OU的外部 ID	
账户关联方式	账户关联
应用状态	启用

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

	「日田会社	idaas-ch-iving fi ving) () () () Web应用	 	★ 投权 洋橋 ▲
	Ω用在⊕	认证你的	第白信息 . 同告	联白信母,子联白
	公田500米県位留	你用約前書醫學特別	2014年11月21日1月1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日	260° (HHAE -) 300°
	查看洋情 修改应用 删除应用	ID an Q40±224bb46		查看应用子账户
		Ingenter Briter		l^{1}
	授权信息	审计信息	API	管理应用内权限
	应用与人员组织的授权关系	查看应用系统详细的操作日志	显否对应用开放系统API	管理应用內菜单与功能权限
	授权	查看日志 查看同步记录	API Key API Secret IP 白名单配置	御定权限系统
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。		
	应用授权			
	应用授权主体主体授权应用			
	应用		账户 组 组织机构 分割	×.
	阿里邮箱	Q	- C Cpid	
	阿甲邮箱测试		ceshi0223	
	MICKIEL ST	,	+ -∪ <u></u> ,	
	阿里邮箱	>		
		共2条 〈 1 〉		
		_		
			保存	
5. 给	该应用配置SCIM			
组	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

SCIM 配置 (阿里邮箱)

账户	组织机构
应用名称	
* SCIM同步地址	https://xxxx.login.aliyunidaas.com/api/application/plugin_alimail/scim/organizat
是否开启	接收同步组织规构的接口,如: http://xxx.com/api/application/scim/organization
协议类型	○ Basic ● OAuth2 应用提供的保护接口的协议类型
* oauth url	https://xxxx.login.aliyunidaas.com/oauth/token oauth url 必填
* client_id	xxxxx client_id 必填
* client_secret	XXXXX
	Chef III. Societ 2/映 保存 取消

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"。

 \times

zwy_test	禹性	\times
常规	2级组	
账户属性	扩展属性	
* 账户名称	zwy_test 账户名称可有会士写字母 小写字母 教字 中划线() 万划线() 卢() 长度至少4.位	
* 显示名称		
邮箱	The second secon	
手机号	□辺, チルラ和節相主少項与一下。 +86 ∨ 请输入有效的手机号	
备注	□透,手机号和邮箱全少填号一个。 管注	
	用户备注信息	//
过期时间	2116年12月31日 可选。不填将使用系统默认过期时间 2116-12-31。	
外部ID		
	提交 取消	

7. 同步组织机构到阿里邮箱

组织架构	查看详情			两位变动 ~	导入 - 导出 - 配置 LDAP 配置钉钉同步
전:22.7180/34026行音谱, 호배可选择组织机, 右眼可 × 기组织机构进行指示。	 第4年 第3日 第3日	Q 类型	目录	状态	操作
	ceshi0223	自識地形形构	Ţ	✓● 共11条 < 1	#改 開步 周歩记录 数00 1 2 > 10 余页 > 数至 2 页
组织机构同步				\times	
组织机构名称: ceshi0223					
说明:本平台作为客户端,向已授权;	的第三方业务系统同步组织机	1构, 需同时满足启用应用	并开启SCIM同步组织机构		
名称 SCI	M配置状态	SCIM同步状态	是否可以推送		
1000					
阿里邮箱 已蘸	音響	已开启	可以推送		
推送方式: API推送					
推送设置: 💿 立即推送 🔵 定时同步					
同步设置: 是否同步子级机构 是	是否同步子级账号				
同步 查看同步记录 取)	首				

8. 同步账户到阿里邮箱

阿里云应用对接·单点和同步数据到阿 里邮箱

组织架构	查看详情					岗位变动 > 导入 > 导出 > 配置 LDAP 配置钉钉同步
在这里对组织来构进行管理。左键可选择组织机构,右键可 × 对组织机构进行循理。	账户 翁 新建账户	目 组织机构 添加成员 ~ 账户	客称 > 请输入账户名称进行搜索	Q. Hote		
cpid	当前账户数 37	/ 已购赛餐规格为 300				
	编号	账户名称	显示名称	类型	目录	操作
	□ 1	zwy_test	zwy_test	自建账户	/ ceshi0223	修改 转的 账户同步 同步记录 移除
	2		_	自建账户	/ ceshi0223	修改 转的 账户同步 同步记录 移除
	3	gc_test	gc_test	自建账户	/ ceshi0223	修改 转商 账户同步 同步记录 移除
						共3条 < 1 > 10銀贝 ※ 誕至 1 页

账户同步

 \times

账户名称: zwy_test

说明:本平台作为客户端,	向已授权的第三方业务系统同步账户,	,需同时满足启用应用并开启SCIM	同步账户。
名称	SCIM配置状态	SCIM同步状态	是否可以推送
			inter and
阿里邮箱	已配置	已开启	可以推送
推送方式: API推送			

同步 查看同步记录 取消

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。

▶ ▶ ▶ ● 里田福 ↔	版			搜索	进入邮箱 帮助中心 postm
概赏	员工帐号管理				
组织与用户 ~					
	新建部门	meite club (14)			
页上版写言理	estato.				
邮件组		新建士的 」 新建的 」 助件组 [设置)	約「王宮 里命名前]		
帐号别名设置		新建帐号 导入导出 > 课	輸入帐号		移动到 过滤帐号 > 权限操作 >
批量设置					
帐号回收站		□ 姓名 ▼	工号 🕶	邮件地址 👻	所屬部门
安全管理		postmaster		postmas= 📑 🖬 🖬	contra state
统计与日志 ~					
企业定制 ~					
邮箱工具 🗸 🗸					
高级应用 ~					

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。

DaaS统一认证身份平台		
欢迎 · IDaaS	我的应用 搜索应用	۹
+0.0		
100 ×	Web应用	
应用管理		
应用子账户		M
设置 へ 我的账户	阿里邮箱测试	阿里邮箱
二次认证	未添加账户	
我的演想		
我的日志	移动应用	
	当前没有将权的移动应用。	
	未找到您需要的应用?可以点由这里 由请应用访问	可权限

您尚未添加该应用的账户关联,请先关联后才能使用.

提示:此应用采用的是手动关联(账户关联),你需要提供正确的用户名,后台管理员审批后才能关联成功;或是管理员直接为你设置 关联 (你能看到此提示表明后台尚无关联纪录)。

子账户*	子账户	
	即您在此应用中的账户	
	提交账户关联	

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。

快速入门		子账户审批 注册审批	应用审批				
应用 应用列表 添加应用 账 ^{pa} 机构及组	~	审批中心 家我中心是 IDaaS 子乐户馆的是单点 审批通过后,用户4	系统中管理员集中处理所有需要审批内容的功能匹 登录可带给应用的身份际吗,如果某正用设置非主 你可以使用子张户单点登到应用系统中,请确认	IIII、当有侍审批项出取时,会在左纲导航三相应位置有数字气场 予张中地就关系为「指个关系」可,用中在影成体出最新的时候 IDaaS用户主持中行子指个的对应关系后的成审批。	雄示。 ,如果没有子预户,则会提交一个子预户绑定申请,出售强	员在此处进行审批。	×
账户管理 分类管理		主账户 (申请人)	子账 ^点 应用名称	待审批 > Q 按索 重要	当前审批如果启用外部审批语,请到外部审批平台进行	行处理!	
WE	^	主账户 (申请人)	子账户	应用名称	申请时间	审批状态	證作
认证原 RADIUS		zwy_test		阿里邮箱测试	2021-06-22 11:28:38	侍审批	查看详情 快速同意 快速拒绝 审批
证书管理							共1条 < 1 > 親至 1 页
援权 权限系统	^						
应用授权							
审计	~						
其它管理	^						
审批中心	2						
消息管理							
会活管理	-						B
我的满思	2						-
若以上步骤全	≧部成功	1完成,用户即可	在用户首页点击阿里邮	箱图标进行访问。			
	我们	1000日 捜索応用	0				

欢迎 · IDaaS						
主导航 ^	Web应用					
首页						
应用管理						
应用子账户		M				
设置						
我的账户	阿里邮箱测试	阿里邮箱				
二次认证						
我的演想						
我的日志	移动应用					
	当前没有接权的移动应用。					
	未找到您需要的应用?可以点击这里 申请应用访问	967 8				

点击上图图标,免密登录到阿里邮箱。

	na ED mi \$5	0 博泰					
	的王即聞	Q 12.R				 _	<i>℃ ↓</i> 50 1
	── 邮件	[25] 日历	2: 通讯录	网盘	[] 笔记	<u></u> 八 群组	
	+ 写邮件	Œ	收件箱-全部(1) ~	编辑			
我	关注的	a Alima 欢迎的 亲爱的	ail 更 用 / • • • • • • • • • • • • • • • • • • 	2020-12-21 开通,邮			
P	收件箱						
P	跟进事项						
\odot	完成事项						
5	重要邮件						
\leq	〕未读邮件						
~ 邮	箱文件夹 十						
Ð	草稿箱						
R	已发送					未选择邮件	
Û	已删除						
\wedge	垃圾邮件						

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

- 以Ⅱ管理员账号登录云盾IDaaS管理平台。具体操作请参考 Ⅱ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
- 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。

 \times

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:

修改应用(阿里云RAM-图形工作站(v1.6林))

	开启控制台时载认分配(产品与服务->访问控制->设置->高级设置->域名管理查看),例如1694154688671682.onaliyun.com。						
* IDaaS IdentityId	https://signin.aliyun.com						
	格式:https://signin.aliyun.com/1694154688671682/saml/SSO,其中1694154688671682为个人综召第一部分内容。						
* SP Entity ID	https://signin.aliyun.com/						
	可在控制台SAML服务提供方元数据中查看,默认与IDaaS IdentityId相同。						
* SP ACS URL(SSO	https://signin.aliyun.com/saml/SSO						
Locationy	默认地址是https://signin.aliyun.com/sami/SSO。						
RelayState	https://gws.console.aliyun.com/						
	登录成功后阿里云跳转地址,以http或https开头。						
AccessKeyID	词输入AccessKeyID						
	AccessKeyID用于进行数据同步,若需要使用同步功能调填写。						
AccessKeySecret	请输入AccessKeySecret						
	AccessKeySecret用于进行数据同步,若需要使用同步功能清填写。						
* NameldFormat	$urn: oasis: names: tc: SAML: 2.0. name id-format: persistent \\ \lor$						
Sign Assertion	No						
* 账户关联方式	● 账户关联 (系统按主子账户对应关系进行手动关联,用户添加后需要管理员审批)						
	○账户映射 (系统自动将主账户名称回划定的字段映射为应用的子账户)						
	提交 取消						

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