



# 应用身份服务 单点登录配置

文档版本: 20211208



## 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。	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。	大意 权重设置为0,该服务器不会再接受新 请求。
⑦ 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。	<ul><li>⑦ 说明</li><li>您也可以通过按Ctrl+A选中全部文件。</li></ul>
>	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 <b>结果确认</b> 页面,单击 <b>确定</b> 。
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 {act ive st and}

## 目录

1.最佳实践	5
1.1. Gitlab对接(SAML)0	5
1.2. Gitlab对接(OAuth2)	5
1.3. JIRA、Confluence、bitbucket对接-使用miniOrange Single Sig 20	0
1.4. JIRA对接-使用SSO 2.033	1
1.5. SAP GUI对接 40	0
1.6. OAuth2对接grafana最佳实践 4	7
1.7. Jenkins对接(SAML) 55	5
1.8. WordPress对接 6	1
1.9. Jumpserver对接-CAS协议60	8
1.10. IDaaS对接Figma实践77	1
1.11. Salesforce对接	4
2.标准协议模板使用指南 9	1
2.1. JWT 模板使用指南	1
2.2. SAML 模板使用指南 11	1
2.3. OAuth2.0模板使用指南 13	7
2.4. C/S(程序)模板使用指南	0
2.5. 表单代填模板使用指南 15.	2
3.主子账户介绍	8

## 1.最佳实践

## 1.1. Gitlab对接 (SAML)

GitLab支持SAML协议的参考官方文档配置: https://docs.gitlab.com/ee/integration/saml.html

Gitlab本地部署可以参考 https://www.cnblogs.com/straycats/p/7637373.html 版本号: gitlab-ce-12.2.1-ce.0.el7.x86\_64.rpm

Gitlab常用命令:

# 启动Gitlab
gitlab-ctl start
# 停止Gitlab
gitlab-ctl stop
# 重启Gitlab
gitlab-ctl restart
# 重新加载Gitlab配置
gitlab-ctl reconfigure
# 查看状态
gitlab-ctl status
# 查看所有的logs
gitlab-ctl tail

### 一、在IDaaS中创建一个SAML应用

1. 在添加应用页面,选择saml应用点击添加

统一认证身份平台	<b>1</b>					消息	默认管理员 → 切换语言	~
概览								
快速入门		添加成	2月 包含了所有已支持的可添加点	田列麦 管理局可以从中选择	<sup>突突接使田的应田进行初始化 鄙害 并开始后途使田</sup>		×	
应用 应用列表	^	✓ 戶(風) 应用分 其提供	为两种: 一种是支持标准的 J 定制化模板进行对接。	WT、CAS、SAML 等模板的	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登录功能;另一种是定制应用,本类应用已经	是供了对接其单点登录	录或用户同步的接口,由 IDaaS 为	
彩加越用	^	saml			٩			
机构及组		应用图标	应用名称	标签	描述	应用类型	操作	
账户管理 分类管理 认证	~	SAML	SAML	SSO, SAML	SAML (Security Assertion Markup Language, 安全新音标记语言, 版本 2.0) 基于 XML 协议, 使用包 含新语 (Assertion) 的安全令牌,在理控区方(DauS) 和四面方(原用)之间的选择份值吧,实现基 于网络原地馆的点语是录。SAML 协议是成熟的认证协议,在国内外的公告云和私有云中有非常广泛的 运用。	Web应用	添加应用	
认证源 RADIUS		salesforce	Salesforce	SSO, SAML, CRM	Salesforce 是在世界范围内广泛使用的公有云 CRM 平台(Customer Relationship Management,客 户关系管理系统)。它为企业提供了事例管理、任务管理、事件动态升极等高效的商业能力。DaaS 支持通过 SAML 协议前点登录到 Salesforce 网站。	Web应用	添加应用	
证书管理 授权	^		WordPress-SAML	SSO, SAML, CMS	WordPress 是全世界最短广泛使用的 CMS (Content Management System, 内容管理系统), 它播 过速带吸水结构并系统和内委自然超频作用的, 六件干万技术或非技术人员生产、管理各种类型的网 线、从成业增热、成功预测行人体需,主题论话、WordPress 所支持的形式非常多样。DaaS 支持 通过 SAML 协议做点登录到 WordPress 网站。	Web应用	添加应用	
权限系统 应用授权		<b>C</b> -J	阿里云RAM-用户SSO	SSO, SAML, 阿里云	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子账户进行访问。	Web应用	添加应用	
分级管理 审计	~	<b>C</b> -J	阿里云RAM-角色SSO	SSO, SAML, 阿里云	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。	Web应用	添加应用	
•								

2. 添加SigningKey

统一认证身	份平台					添加应用 (SAML)		1 占主沃加(	ianinaKey	
<b>既览</b> 央速入门		↓ 本页 应用 其提	面包含了所有已支持的可添加 分为两种:一种是支持标准的 供定制化模板进行对接。	应用列表,管理员可以从中选择 3 JWT、CAS、SAML 等模板的	<sup>8希望使用的应用进行初始化</sup> 应用,在这里可以通过添加外	导入SigningKey 漆	b⊡SigningKey	TX AND DOD	2、添加完/	成之后
成田	~					別名	序列号	有效期	秘钥算法	-
应用列表						CN=测试, ST=1, C=CN	8951765930467520667	180	RSA	102
添加应用		应用图标	应用名称	标签	描述					
账户	^		C/S程序	CS, PC, OIDC	唤醒程序后通过OIDC协议					
账户管理		~	C/S程序(浏览器)	CS, PC, Multi Browser	唤醒指定浏览器打开指定 (IE/谷歌/火狐/搜狗/360等					

3. 创建SAML应用 配置参数可以先随意填写,之后还要进行修改

添加应用(SAM	AL)	×
应用ID	idaas-cn-beijing-3bohwti7lfkplugin_saml1	
* 应用名称	SAML	
* IDP IdentityId	1 IDP IdentifyId is required	
* SP Entity ID	1	
	SP Entity ID is required	
<ul> <li>SP ACS URL(SSO Location)</li> </ul>	http://www.sosc.com	
* NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:transient	~
* Binding	POST	~
SP 登出地址	请输入SP 登出地址	
Assertion Attribute	Assertion Attribute key - +	
Oire Annahire	断言属性。设值后,会将值放入SAML断言中。名称为自定义名称,值为账户的属性值。	
Sign Assertion		
IDaaS发起登录地址	IDaaS发起登录地址 以 http://、 https:// 开头, 填写后使用 iDaaS 发起登录将会跳转到该地址, 而不会使用 SAML 的idp发起登录流程	
* 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描定的字段映射为应用的子账户)	
	提交取消	
修改gitla	b配置文件	

### 囗 注意

在修改配置时请将下面的注释删除,避免gitlab配置格式的影响

#### vim /et c/git lab/git lab.rb

```
#允许用户使用SAML进行注册而无需手动创建账户
gitlab_rails['omniauth_enabled'] = true
gitlab_rails['omniauth_allow_single_sign_on'] = ['saml']
gitlab_rails['omniauth_block_auto_created_users'] = false
#设置自动将SAML用户与现有的GitLab用户连接
gitlab_rails['omniauth_auto_link_saml_user'] = true
#添加提供程序配置
gitlab_rails['omniauth_providers']=[
{
   name: 'saml',
   args: {
      #gitlab的断言地址,标绿部分替换为gitlab实际的地址
          assertion_consumer_service_url:'http://192.168.20.178/users/auth/saml/callback',
      #证书的指纹信息,在IDaaS配置SAML应用后获取
         idp_cert_fingerprint:'a9:68:15:e2:35:3f:1e:de:ea:ac:26:62:a3:88:aa:9c:62:4e:e7:8a',
      #固定格式,http://192.168.20.173:8080为IDaaS域名地址,lin1121samlIDaaS中对应的saml应用ID,请根据实
际信息进行调整
         idp_sso_target_url:'http://192.168.20.173:8080/enduser/api/application/plugin_saml/lin1121saml
/sp_sso',
      #一般为固定格式,可以在gitlab登录页获取
         issuer: http://192.168.20.178/users/auth/saml',
         name_identifier_format:'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',
       },
   #标签,可以根据需要随意更改
   label:'IDaaS'
}]
```

#### 各参数具体获取方法如下

• assertion consumer service url获取方式如下:

🤟 GitLab Projects ~ Groups ~ More ~ 🖉	1 <u>_</u>			<b>Đ</b> ~	Se
& Admin Area	Admin Area > Applications				
BE Overview	System OAuth applications				
L1 Analytics	System OAuth applications don't belong to	any user and can only be managed by admin	5		
😨 Monitoring	New application				
📢 Messages		点击新建	<b>C</b> linete	•	6-1
🕹 System Hooks	Name Caliback UKL		Clients	No	No
R Applications	Samor		0	10	NO
Abuse Reports     0					
🔎 Deploy Keys					
Service Templates					
	olications				
© Appearance	plications				
Settings					

🦊 GitLab Projects 🗸 (	Sroups 🗸 More 🖌 🌽		C v Search or jump to Q D 1
🐉 Admin Area	Admin Area > /	Applications	
BE Overview	New applic	ation	
Le Analytics		Name	
Monitoring		Redirect URI	↓ 埴写·gitlab地址/users/auth/saml/callback
📢 Messages			
🕹 System Hooks		Trusted	Trusted applications are automatically authorized on Gitl ab OAuth flow. It's highly recommended for the security of users that trusted applications have the
B Applications			confidential setting set to true.
Abuse Reports		Confidential	The application will be used where the client secret can be kept confidential. Native mobile apps and Single Page Apps are considered non-confidential.
℅ Kubernetes		Scopes	Grants complete read/write access to the APL including all groups and projects, the container registry, and the package registry.
Deploy Keys			□ read_tuter
Service Templates			Grants read-only access to the authenticated user's profile through the /user API endpoint, which includes username, public email, and full name. Also grants access to read-only API endpoints under /users.
Labels			Grants read and Grants read access to the API, including all groups and projects, the container registry, and the package registry.
2 Appearance	全部勾	J选	ead r pository
Settings			Grantsread-only access to repositories on private projects using Git-over-HTTP or the Repository Files APL
			Grants read-write access to repositories on private projects using Git-over-HTTP (not using the API).
			Grants permission to perform API actions as any user in the system, when authenticated as an admin user.
			openic     Grants permission to authenticate with GitLab using OpeniD Connect. Also gives read-only access to the user's profile and group memberships.
≪ Collapse sidebar			Grants read-only access to the user's prome data using Openio Connect.
H Gill ab Projects	× Groups × More × 🌶		😫 🖌 - Saarch or in
& Admin Area		Admin Area > A	pplications
E Overview		() Applica	tion was successfully updated.
Lu Analytics		Application	n: SamlGit
👳 Monitoring		Application	ID 3c77ec91 🔓
📢 Messages			
ل System Hooks		Secret	8c9e961;
B Applications		Callback UR	L http:
Abuse Reports	0	Trusted	N
Kubernetes		Confidentia	I N
O Deploy Krist			<ul> <li>api (Access the authenticated user's API)</li> <li>read user (Read the authenticated user's name and information)</li> </ul>
- Depioy Keys			read_paper(Read Apri)     read_paper(Read Apri)     read_paper(Read Apri)
Service Templates		Scopes	<ul> <li>read_repository (vinces read-only access to the repository)</li> <li>write repository (Allows read-write access to the repository)</li> <li>write (Order a 6) content of the repository)</li> </ul>
Labels			<ul> <li>suco (renorm Ari actions as any user in the system)</li> <li>openid (Authenticate using OpeniD Connect)</li> </ul>
Appearance			<ul> <li>prome (vinows read-only access to the user's personal information using OpeniD Connect)</li> <li>email (Allows read-only access to the user's primary email address using OpenID Connect)</li> </ul>
Settings			
		Edit	Jestroy

- idp\_cert\_fingerprint获取方式如下:
- 1、导出证书

取消

确定

添加应用 (SAML) 概度 快速入门 添加应用 别名 点川利本
 点川利本
 ス加助用
 初次日本
 利次日本
 分供管理
 八正
 八正原
 RADIUS
 送刊管理
 利収
 利収
 利収
 利収
 利収
 大回来
 大回来
 大回来
 大回来
 大回来
 大回来 CN=測試 ST=1, C=CN 选择 导出 选择之前创建的SigningKey,点击导出 S salesforce (-) (-) 國它管理 M  $\times$ 导出SigningKey 可以用不同的文件格式导出 SigningKey • DER 编码二进制 X.509(.CER)(D) Base64 编码 X.509(.CER)(S)

#### 在添加应用界面,选择saml应用模板,点击添加应用。选择之前创建的SigningKey,点击导出

#### 2、查看指纹。

打开证书,点击详细信息-指纹获取指纹。每两个数字后面加上一个冒号:,跟文档的格式保持一致。

#### △ 警告

每两个数字后面加上一个冒号":",否则将报错。

<ul> <li>第规 详细信息 证书路径</li> <li>显示(S): &lt;所有&gt;</li> <li>字段 值</li> <li>③ 签名哈希算法 sh</li> <li>③ 颁发者 1,</li> <li>③ 有效期从 20</li> <li>③ 可到 20</li> <li>③ 使用者 1,</li> <li>④ 公钥 85</li> <li>④ 公钥参数 05</li> <li>● 指纹 25</li> </ul>	✓ i na1 1, CN 019年9月24日 16:07:57 019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
显示(S): < <u>所有</u> > 字段 □ 签名哈希算法 □ 颁发者 □ 須效期从 □ 20 □ 有效期从 □ 20 □ 使用者 □ 1, □ 20 □ 使用者 □ 20 □ 使用者 □ 3 20 □ 使用者 □ 3 20 □ 1, □ 3 20 □ 3 0 5 1, □ 3 20 □ 3 20 20 20 20 20 20 20 20 20 20	→ a1 1, CN 019年9月24日 16:07:57 019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
字段     値       圖 签名哈希算法     sh       圖 颁发者     1,       圖 有效期从     20       圖 有效期从     20       圖 使用者     1,       □ 公钥     85       □ 公钥     85       □ 指紋     a9       a96815e2353f1edeeaac2662a38	a1 1, CN 019年9月24日 16:07:57 019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
字段       値         圖 签名哈希算法       sh         圖 颁发者       1,         圖 有效期从       20         圖 列       20         圖 使用者       1,         圖 公钥       R9         ●公钥参数       05         圖 指紋       a9	Ana1 1, CN 019年9月24日 16:07:57 019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
<ul> <li>□ 签名哈希算法</li> <li>□ 颁发者</li> <li>1,</li> <li>□ 有效期从</li> <li>20</li> <li>□ 可如期人</li> <li>20</li> <li>□ 使用者</li> <li>1,</li> <li>□ 使用者</li> <li>1,</li> <li>□ 公钥</li> <li>□ 公钥</li> <li>□ 公钥</li> <li>○ 公钥参数</li> <li>○ 公钥</li> <li>○ 公</li> <li>○ 公钥</li> <li>○ 公</li> <li>○ ○</li> <li></li></ul>	ha1 1, CN 019年9月24日 16:07:57 019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
<ul> <li>□ 颁发者</li> <li>1,</li> <li>□ 有效期从</li> <li>20</li> <li>□ 到</li> <li>□ 使用者</li> <li>1,</li> <li>□ 公钥</li> <li>□ 公钥</li> <li>□ 公钥</li> <li>□ 公钥</li> <li>○ 公钥参数</li> <li>○ 公钥参数</li> <li>○ 15e2353f1edeeaac2662a38</li> </ul>	1, CN 019年9月24日 16:07:57 019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
<ul> <li>□ 有效期从 20</li> <li>□ 到 20</li> <li>□ 使用者 1,</li> <li>□ 公钥 R3</li> <li>□ 公钥 R3</li> <li>□ 公钥 80</li> <li>□ 指纹 a5</li> </ul>	019年9月24日 16:07:57 019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
<ul> <li>□ 到 20</li> <li>□ 使用者 1,</li> <li>□ 公钥 R\$</li> <li>□ 公钥参数 05</li> <li>□ 指纹 a9</li> </ul>	019年10月24日 16:07:57 1, CN SA (1024 Bits) 5 00
<ul> <li>□●使用者</li> <li>□○公钥</li> <li>□○公钥参数</li> <li>○○公钥参数</li> <li>○○公</li> </ul> <ul></ul>	1, CN SA (1024 Bits) 5 00
◎公钥 R: ◎公钥参数 05 ◎指纹 a9 a96815e2353f1edeeaac2662a38	SA (1024 Bits) 5 00
○ 公钥参数 05 ● 指纹 a9 a96815e2353f1edeeaac2662a38	5 00
■指纹 a9 a96815e2353f1edeeaac2662a38	
a96815e2353f1edeeaac2662a38	96815e2353f1edeeaac2
a96815e2353f1edeeaac2662a38	~
a90615e2555fTedeeaac2002a56	90-62479-
	8aa9c024ee78a
	编辑属性(E) 复制到文件(C)

● idp\_sso\_target\_url获取方式

く上一页 1

概述		应用列表		应用详情(g	jit_test)			
快速入1 应用 应用	」 	应用列表 ◎  「 ●  ●  ●  ●  ●  ●  ●  ●  ●  ●  ●  ●  ●	広用可以交現単立登録和数編明歩戦力。	应用Uuid	b6b3b9a9f18c29894244a0d48f68df8bH8LhsKzdhPR			
源加	喧用	anduranan, <u>andravan</u> tander indere. #	Chernal Jack, comartyr, picaramanyshranys, an	SigningKey	12210798747(CN=git_test)			
机林	2及坦 - 管理	6#8% 6#2#	<u> </u>	应用详述情	u nes.tc:SAML.2.0.nameid-format transient http: 96.8929/users/auth/saml/callback			
9\$ 认证	4管理	S. git_test	idaas-cn-beijing-3bohwti7/tkplugin_saml	IDP IdentityId	git_test i PAML 元配置文件			
143 RA	EM DIUS	应用信息	认证信息	SP Entity ID	ers/auth/saml			
证 <del>1</del> 授权	5管理		应用的单点登录地址	Binding Sign Assertion	POS1			
权用	見系統 目接収	THE REPORT OF CALLER	IDaaS发起地址	Assertion Attribute	۰. <del>ت</del>			
审计		接权信息	审计信息	IDaaS发起整要地	ż			
異它管?	e v	MUTH-6人GAMES GENERACIES 接保	重和近月第380年和11日本。 查看日本 查看局步记录	SP波起地址	htt. m/enduser/api/applicatio SAMLRequest=>>>>>&RelayState=yyy	on/plugin_samilid milsp_sso		
		J TEST1	注意:和置	文件中填:	高地的方法。SAMLRequestESP发起所原带的参数。以来 写http,不是htt	第159年: RelayState是SSO回的目标URL参数, 已实现功策 DS		
				应用状态 账户关联方式	截用 账户关款			
(	② 说明							
I	lDaaS域	名地址可以在 <mark>云盾</mark> II	DaaS管理控制台获取	l.				
I	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	pi.aliyunidaas.com		

#### • issuer获取方式如下:

- → C ① 不安全   192.168.20.178/users/sign_in				아 월 ☆	r e
	Open source software to collaborate on code	Sign in	Register		
	Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge requests. Each project can also have an issue tracker and a wiki.	Username or email			
		Password			
		Remember me	Forgot your password?		
	鼠标放上去时,会在左下角显示url地址	Si	gn in		
		Sign in with IDaaS			
		- remember me			
69.20.179/urger/auth/caml	Explore Help About GitLab				

#### 修改完配置之后,在命令行中输入以下命令重启gitlab,刷新配置信息

gitlab-ctl stop gitlab-ctl reconfigure gitlab-ctl start

## 三、修改saml应用配置

修改saml应用配置如下

← 选择signingKey		$\times$
* 应用名称	gitlab	^
* 应用类型	✔ Web应用	
* IDaaS IdentityId	IDaaS_test 唯一标识 IDaaS IdentityId is required	
* SP Entity ID	识别SP的标识,即Issuer的值 http://192.168.20.178/users/auth/saml SP Entity ID is required	
* SP ACS URL(SSO Location)	http://192.168.20.178/users/auth/saml/callback gitlab的断言地址	
SP 登出地址	请输入SP 登出地址	
* NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent 选择与文档中的配置的相同即可	J
* Binding	POST ~	
* SP登录方式	应用自定义登录页 ~	
Sign Assertion	No	
* 账户关联方式	<ul> <li>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)</li> <li>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)</li> </ul>	

## 四、设置Gitlab对应账户标识(IDaaS中的子账户)

使用root账户登录,为账户添加账户标识

🦊 GitLab Projects ~ Groups ~ More ~ 🖋		<b>.</b> ~	Search or jun
Admin Area	Admin Area > Users > Administrator		
BE Overview	Administrator (Admin)		
Dashboard Projects	Account Groups and projects SSH keys Identities Impersonation Tokens		
Users 2 Groups 2	Administrator 点击Identities		
Jobs Runners			
Gitaly Servers	Profile page: root		
Lu Analytics	Profile		
😔 Monitoring	Member since Feb 24, 2021 8:20am		
<b>⊄</b> Messages	Account:		

#### 应用身份服务

₩ GitLab Projects ×	Groups Y More Y 🌶 C Y Search or jump to Q D	Г
🐉 Admin Area	Admin Area > Users > Administrator > New Identity	
BE Overview	New identity	
네 Analytics		
🚇 Monitoring	Provider (DaaS (sami)	*
📢 Messages	Identifier GC_asdfd	
ل System Hooks		
Applications	weedings 复向,这主即 <u>为</u> 应用于顺广	
Abuse Reports		
℅ Kubernetes		
🔎 Deploy Keys		
E Service Templates		
Zabels		
P Appearance		
🗘 Settings		
Gill ab Brojectr X G	By Conscharge tame to D D the F2	
Admin Area	Admin Area > Uses > Administrator	
BE Overview	Administrator (Admin)	
네 Analytics		
Monitoring	Account Groups and projects SSH keys Identities Impersonation Tokens	
📢 Messages	Provider Identifier New identity	
🖞 System Hooks	IDaaS (saml) GC_asdfd Edit Delete	
B Applications		
Abuse Reports     0	将这个作为应用子账户与IDaas中账户关助	ŧ
₲ Kubernetes		•
🖉 Deploy Keys		
Service Templates		
Zabels		
Appearance		
Settings		

## 五、IDaaS添加子账户

点击应用详情,查看应用子账户。

概范		应用列表						
央連入门			の用別事					×
业用 <b>应用列表</b> 添加应用		Ŷ	201773名 管理员可以在当前页面管理已经添加的所有应用,应用可以实现单点 当添加完应用后,应该确认应用处于自用状态,并已经完成了接权,有	登录和数据同步能力。 至应用详情中,可以看到应用的详细信息、单点登录地址、子别	:戶配置、同步配	显、接权、审计等信息。		
低户	^	添加应用	请输入应用名称		Q			
形向管理		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		S.v.	git_test	idaas-cn-beijing-3bohwti7ifkplugin_saml	Web应用			援权 详情 🔺
以证原 RADIUS	^	应用	信息	认证信息		账户信息 - 阿步	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、组同步推送至应用	平台主账户与应用系统中子账户目	的关联表
受权 权限系统	^	22	洋橋修改应用 影除应用	IDaaS发起地址		同步机构 SCIM配置	查看应用子账户	
应用授权 單计	~	授权	信息	审计信息		API	普理应用内权限	
民它管理	~	应用	与人员组织的提权关系	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	
兒園	ř	授权		查看日志 查看同步记录		API Key API Secret	绑定权限系统	
		$\mathbf{J}_{_{\mathrm{PWY}}}$	TEST1	idaas-cn-beijing-3bohwti7ifkplugin_jwt	Web应用			授权 详情 ▼
							共2条 〈 1 〉	10 条页 > 第至 1 页

点击添加账户关联

(-) 阿里云					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	App 区 🗘 👾 🕜 簡体
UZ.	应用列表 / <b>子账户</b>							
注意入门 川 へ	← 子账户						泽加	第中关联 批量导入 批量号:
应用列表 添加应用 (户 ^ 机构及组 () → () → () → () → () → () → () → () →	子账户 子账户指的最石損 単例: IDaaS 中利 账户关联方式: 6	首定应用系统中,用户会以什么身份进行 有主账户 张三(用户名 zhangsan),在 丘应用创疆时,如果选择了账户缺时,即	访问,主张户描的是 IDaaS 中的账户。 企业的 BPM 应用系统中,这个用户的 默认主张户和子账户完全一致,无需数	在进行单点登录时,IDaaS 会向应用那 用户名量 agoodman,即子账户应为 ag 置。如果选择了账户关联,则需要在这	系统传递对应的子账户,读子账户需要在 goodman,与主账户 zhangsan 进行关期 重进行手动的子账户创建和主子账户关键	边用系统中存在且可识别。 t. 团。		>
账户管理 分类管理	git_test							
○征 ^ 认证原	主账户 (账户名称)			Q				
RADIUS	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
证书管理				Æ	已关联	无	2021年2月24日	<del>激</del> 的
权 へ 权限系统 应用授权							共1条	( 1 ) 跳至 1 页

主账户为IDaas中的账户,子账户为刚刚Gitlab中设置的 identity.

添加账户关联	
* 主账户	gc_test
* 子账户	GC_asdfd
	保存 返回

完成以上步骤,即可单点登录到git lab。

### FAQ

1. 显示下图报错

## SAML-gitlab 访问异常

## 当前账户无子账户,请联系管理员添加或在应用子账 户处申请!

gitLab的identifier和应用下设置的子账户需要一致。

2. 使用同步进入gitlab的账户进行登录,提示邮箱不能为空。

方法1: 绑定主子账户时,子账户直接使用用户名,不使用邮箱;

)

#### 方法2:在IDaaS中,修改SAML应用添加邮箱参数

修改应用 (SAML-Gitlab12)

*NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	~
* Binding	POST	~
	SAML协议中规定的Binging方式,不同的Binding方式使用不同的通信方式和消息体,常用方式是SP使HTTP Redirect Binding通过浏览器将SAMLRequest转发到IDP的SSO地址,IDP使用HTTP POST Bin式将用SAMLResponse返回到SP的ACS地址。	9用 ding7
SP 登出地址	请输入SP 登出地址	
	需要SP提供,用于IDP告知应用是否登出成功,在SP操作退出后,会跳转IDP并注销IDP会话,并从ID 到该地址。	P跳车
Assertion Attribute	email 邮箱 ~ 一 +	
	断言属性。设值后,会将值放入SAML断言中。名称为自定义名称,值为账户的属性值。	
Sign Assertion		
	定台对断言进行佥名,通常可以个用升后。	
IDaaS发起登录地址	IDaaS发起登录地址	
	以 http://、 https:// 开头, 填写后使用 IDaaS 发起登录将会跳转到该地址, 而不会使用 SAML 的idp发起	<b>建</b> 录流

## 1.2. Gitlab对接 (OAuth2)

Gitlab常用命令:

# 启动Gitlab
gitlab-ctl start
# 停止Gitlab
gitlab-ctl stop
# 重启Gitlab
gitlab-ctl restart
# 重新加载Gitlab配置
gitlab-ctl reconfigure
# 查看状态
gitlab-ctl status
# 查看所有的logs
gitlab-ctl tail

### 一、在IDaaS中创建一个OAuth2应用

点击导航栏中点击添加应用,选择OAuth2应用模板

#### 单点登录配置·最佳实践

统一认证身份平台												;	68 ઉ	默认管理员▼	切换语言 ~
概次	添加应用	B													
快速入门	全部	标准协议	定制模板												
应用 ^ 应用列表 添加应用 账户 ^	Ŷ	添加应用 本页面包含 应用分为网	】 含了所有已支持的可添加应 5种:一种是支持标准的 J	用列表,管理员可以从中选择 WT. CAS. SAML 攀横微的点	继希望使用的应用进行初始/ 应用,在这里可以通过添加	化配置,并开始后续使用。 对应的标准应用模板未实现单点3	·登录功能;另一种基定)	制应用,本美应用已经都	皇供了对接触单点要录成用	8户周纱的搬口,由 ID:	aaS 为展摄供定物代	2欄板进行对接。			×
机构及组	oauth2						Q								
球户管理 分类管理	应用图	lik.	应用名称	标签	描述			-				廢	用类型		操作
认证 ^	0		OAuth2	OAuth2	OAuth 是一个开放的资源	源摄权协议,应用可以通过 OAu	uth 获取到令牌 access_	_token,并携带令牌来新	Q务铸造求用户资源。应用	目可以使用 OAuth 应用	掌板来实现统一身份	<b>信理。</b> w	eb应用	)	添加应用
RADIUS 证书管理											÷	共1条 〈	1	10 魚页 ~	親至 1 页
权限系统															
应用授权 分级管理															
审计 ~															
其它管理 															
	© 2014-20	019 IDaaS													版本:1.5.7
l															
添加应用(	OAuth	12)													$\times$
💡 OAut	th2 应用	1.只实现	7 SP(Serve	r Provider, 业终	务系统方) 发起	的单点登录流程	₽.								
				_											
应用图标															
			OAU	гн											
			◎ 上传	文件											
			图片大小不	超过1MB											
应用ID			lin1121oau	uth23											
* 应用名称			OAuth2												
÷0.000			_												
* 应用类型			Web <u>(w)</u>	∄											
			"Web应用" 显示 如馬	和"PC客户端"」 目在タイ环语	」只会在用户We 和都显示应用	eb使用环境中显 I叫勾洗多个	示,"移动应	7月"只会在月	目户客户端中	显示,"数据	铜步"应用	1只用作数	据的同	司步不会在	用户侧
			TENN YEAR	9241134   X1990	ST REAL OWNER OF	IX3-SKEDP 1 6									
* Redirect UR	d		http://www	w.xxx.com/use	ers/auth/IDaaS	5/callback									
			OAuth2 Re	direct URI, htt	tp / https or AF	PP-Scheme.									
SP HomePa	adeURI														
			应田首百州	까 구분국과	145-12000										
				ML, X1 <del>51</del> -MI											
* GrantType			authoriza	tion_code											~
L			Authorizati	on_Code: 授	权码模式 (即)	先登录获取Cod	le,再获取Tok	ken),标准	ŧOAuth2流程	; Implicit:	简化模式	; (在Red	irect_u	uri的Hash	传递To
			ken) 适用	于验证第三方台	合法性时使用;	;									
Access T-1	on the	788	7000												
ACCESS_10K	(11)月30	CAN .	7200		12 Million and 1										
			Access_To	Ken的有效时也	长(単位:秒),	默认为/200(2小	\und 1)								
Refresh Tok	en有效	期	604800												
	-		Refresh To	)ken的有效时+	长(单位:秒)。	默认为604800/7	7天)。								
			提交	取消											

添加应用需要填写两个参数,Redirect UR和GrantType Redirect URI填写格式如下:Gitlab\_url/users/auth/IDaaS/callback。 其中Gitlab\_url为gitlab服务器的地址,IDaaS为在Gitlab服务器配置文件里配置的标识。 GrantType选择Authorization\_Code(授权码模式)

### 二、修改gitlab配置文件

(在修改配置时请将下面的注释删除,避免gitlab配置格式的影响)

vim /etc/gitlab/gitlab.rb

```
#允许用户使用oauth2进行单点登录
gitlab_rails['omniauth_enabled'] = true
gitlab_rails['omniauth_allow_single_sign_on'] = ['oauth2_generic']
gitlab_rails['omniauth_block_auto_created_users'] = false
#添加提供程序配置
gitlab_rails['omniauth_providers'] = [
ł
  'name' => 'oauth2_generic',
  #IDaaS中OAuth2应用的client_id和client_secret
   'app_id' => 'oauth_client_app_id',
   'app_secret' => 'oauth_client_app_secret',
   'args' => {
     client_options: {
      #IDaaS服务器的地址
      'site' => 'https://your_oauth_server',
      #IDaaS提供的获取用户信息的接口
      'user_info_url' => '/api/bff/v1.2/commons/user_details',
      #IDaaS提供的获取token的地址
      'token_url' => '/oauth/token'
     },
    user_response_structure: {
     root_path: ['data', 'udAccountInformation'],
     attributes: { nickname: 'username' }
    },
    #标签名,可以随意填写,但需要和创建OAuth2时填写的标识统一
    name: 'IDaaS',
    strategy_class: "OmniAuth::Strategies::OAuth2Generic"
 }
}]
```

oauth\_client\_app\_id和oauth\_client\_app\_secret获取方式如下: 选择步骤一创建的OAuth2应用,点击查看详情

#### 单点登录配置·最佳实践

统一认证身份 <sup>5</sup>	平台					消息 🕠 🛛 默认管理员 -	切换语言 ~
概念 快速入门		应用列表 1、点击应用列表,查看所有应用					添加应用
应用 应用列表	Ŷ	○ 加州列表 管理内可以在川航页周智理已经添加的所有应用,应用可以实现自 当添加完成用后,应该确认应用处于应用状态,并已经完成了程序	加登录和 用户同步 能力。 。在应用详情中,可以看到应用的详细信息、单点登录地址、子张升	"配蓝、同步配蓝、接权、审计等信息。			×
液加亚用 账户	^	请输入应用名称		Q	2、选择创建好的OAut	h2应用,点击详情	
机构及组 账户管理		应用图标 应用名称	₿₩0	设备类型	应用状态	操作	
分樂管理		OAuth2	lin1121oauth22	Web应用		授权 详情 🔺	
认证 认证源 RADIUS	^	应用航意	账户信息 - 同步	接权信息	明行十代的		
证书管理		应用的详细信息 (熱用后可編輯)	SCIM协议设置以及把组织机构、组同步推送至应用。	应用与人员组织的授权关系	查看应用系统详细的	温作日志。	
授权 权限系统	^	前光展画	同步机构 SCIM配置	授权	查看日志 查看	同步记录	
应用授权 分级管理		3、点击查看详情					
审计	~	应用Xt分词用的APH设口					
其它管理 <sup>●</sup> 设置	× ×	API Key API Secret					
		SAP GUI	lin1121cs_sap_gui	PC客户路		授权 详情 ▼	
		WordPress-SAML	lin1121wordpress_saml	Web应用	$\checkmark$	授权 详情 ▼	

#### 应用详情 (OAuth2)

应用图标



应用ID	lin1121oauth22
应用名称	OAuth2

Client Id	3eb0fd2f4ac24170c3e009b6845592b66nLV5ghbUyi
Client Secret	l4v6JAUAbH3gx7gp4XGKh9wTt4Dbq3hueTEFdkY01b
Redirect URI	http://47.93.214.172/users/auth/IDaaS/callback
SP HomePageURL	
GrantType	authorization_code
Authorize URL	https://lin1121.idp4.idsmanager.com/oauth/authorize?re
	6nLV5ghbUyi&redirect_uri=http%3A%2F%2F47.93.214.
Access_Token有效期	7200秒
Refresh Token有效期	604800秒
应用状态	启用
创建人	admin
创建时间	2019-12-05 10:24

修改完配置之后,在命令行中输入以下命令重启gitlab,刷新配置信息。

gitlab-ctl stop gitlab-ctl reconfigure gitlab-ctl start

重启完成之后,可以在gitlab登录界面如下:

<b>₩</b>				
GitLab Community Edition				
Open source software to collaborate on code	Sign in	Register		
Manage Git repositories with fine-grained access controls that keep your code secure. Perform code reviews and enhance collaboration with merge	Username or email	Username or email		
requests. Each project can also have an issue tracker and a wiki.				
	Password			
	Remember me	Forgot your password?		
		Sign in		
	Sign in with	_		
	I Daa S			
	Remember me			

## 三、账户关联

用户登录gitlab之后,在setting-Account中点击Connect进行账户关联

🦊 GitLab Projects 🗸 Groups 🗸 Activity Milestones Snippets 🖿		C v Search or jump	on	6 9	~ 🙆 •	Â
User Settings	User Settings > Account		lin003			
Profile  Account  Applications	Two-Factor Authentication Increase your account's security by enabling Two-Factor Authentication (2FA)	Status: Disabled Truble two-factor authentication 1、进入设置	Set status Profile Settings			
P Chat 2、选择账户	Social sign-in	Connected Accounts	Sign out			
Access Tokens     Emails	Activate signin with one of the following services	Click on icon to activate signin with one of the following services I Daa S Connect 3、进行账户关联				
A Password	Change username	Path				
A Notifications	Changing your username can have unintended	http://47.93.214.172/ lin003				
₽ SSH Keys	side effects, Learn more.	Current path: http://47.93.214.172/lin003				
₱ GPG Keys		Update username				
# Preferences	Delete execut	Delating an associat has the following offects:				
Active Sessions	Delete account	Certain user content will be moved to a system-wide "Ghost User" in order to maintain content				
Authentication log		for posterity. For further information, please refer to the user account deletion documentation.				
47.93.214.172/lin003						v

跳转到IDaaS的登录界面,使用IDaaS的账户进行登录



登录成功之后页面会切换回Gitlab的页面,并在页面上方出现一条提示信息

ILAD Projects ~ G	roups 🗸 Activity Milestones Snippets 🖿		🗄 🗸 Search or ju
User Settings		User Settings > Account	
Profile		Authentication method updated	
a Account		Two-Factor Authentication	Status: Disabled
# Applications		Increase your account's security by enabling	Enable two-factor authentication
D Chat		Worractor Authentication (2PA)	
Access Tokens		Social sign-in	Connected Accounts
🖾 Emails		Activate signin with one of the following	Click on icon to activate signin with one of the following services
A Password		services	I Daa S Disconnect
A Notifications			5.1
₽ SSH Keys		Change username	Path
👂 GPG Keys		Changing your username can have unintended side effects. Learn more.	http://47.93.214.172/ lin003 Current path: http://47.93.214.172/in003
章 Preferences			Update username
Active Sessions			
Authentication log		Delete account	Deleting an account has the following effects:
			<ul> <li>Certain user content will be moved to a system-wide "Ghost User" in order to maintain conten for posterity. For further information, please refer to the user account deletion documentation</li> </ul>
			Delete account

通过以上步骤,完成使用OAuth2应用模板实现Gitlab的单点登录。

## 1.3. JIRA、Confluence、bitbucket对接-使用 miniOrange Single Sign On

本文为您介绍如何通过SAML协议单点登录到JIRA, Confluence或者bitbucket,实现应用的快捷登录,提升员工办公体验。我们此处演示的是单点登录到阿里云控制台

#### 背景信息

某些企业员工日常办公需访问JIRA, Confluence 或者bitbucket,每次都需要访问应用的登录地址,输入账 户名,密码登认证方式进行登录,如果有多个类似应用,就需要记录多套密码,使用应用时繁琐和耗时。

#### 解决方案

IDaaS应用身份服务通过账户单点登录到JIRA, Confluence或者bitbucket, 只需要登录一次, 就可以看到所 有有权限访问的应用, 并对应用进行单点登录。

JIRA, Confluence 和 bit bucket 配置步骤一样,都使用下面的操作步骤进行配置。

#### 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. 在左侧导航栏,点击 应用 > 添加应用,选择SAML应用模板,点击添加应用。

快速入门		全部 标准协议	定制模板							
应用	^									
应用列表		25 April	-							×
添加应用		(would b) (								
账户	~	应用分)	的两种:一种是支持标准的 JV	NT、CAS、SAML 等模板的 8	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的接口,由 IDaaS 为其提供定制化模板近	时对接。			
机构及组										
账户管理		SAML				Q.				
分类管理		应用图标	应用名称	应用ID	标签	描述	应用类型	17	Rff=	
认证	~	63	RE-PAM. HOSEO	plugin aliaun	990 94MI 1787	基于 SAML 协议,实现由 IDaaS 单点整录到阿里云控制台;使用该模板,需要在RAM中为每个用户单独创建RAM子账户,IDaaS账户和RAM子账	Web <sup>位田</sup>		Fands FR	
认证瞭			P34220000110 0000	progni_anyon	GOO, ORME, PEAKER	户通过缺时实现单点整要到RAM。	WOMALPH	10	A00412.PE	
RADIUS 征书管理		[-]	阿里云RAM-用户SSO	plugin_aliyun_role	SSO, SAML, 阿里云	著于 SAML 协议,实现由 IDaaS 单心理说到何里云控制台:使用读微观,需要RAM中创建RAM角色,不需要方每个用户单级创建RAM子现户, IDaaSILF中GRAM指色通过纳封实现单点包录到RAM,	Web应用	18	助应用	
授权权限系统	^	S	SAML	plugin_saml	SSO, SAML	SAML (Security Assertion Markup Language, 安全新宣历记录室, 版本 2.0) 基于 XML 协议,使用包含新宣(Assertion)的安全令牌,在接权为 (Daas5) 和国最方(应用) 之间伸起身份信息,实现最于网络静地的单点型是。SAML 协议是成果的认证协议,在限小外给公会实际机构实中有非 第二经验证用。	Web应用	18	助应用	
应用接収	÷	W	WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress 是全型界最初了运用的 Edds(Content Management System,内容管理系统),它邀往非常误大的操作系统的分便目前的进行界景, 分许于方法水或和技术人员生产,管理性特殊型的网络。从奥亚网站,政府对面到个人募集,主面论由,WordPress 所交给给完过和某单称,IDaa 艺术者型 SAML WordPress 网站。	3 Web应用	18	助应用	
其它管理	~	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 IDaes 我阿爾斯納帕帕德克發展和用戶同步,	Web应用	18	師应用	
设置	Ť					共5条	< 1 >	10 祭/页 >	E 1	

#### 添加SigningKey

						0	
	添加应用(SAML)						$\times$
	导入SigningKey	添加SigningKey					
	别名	序列号	有效期	秘钥算法	算法长度	操作	
现单点登录功			暂无数据				
实现由 IDaaS 急登录到RAM。							
<sub>实现田</sub> IDaaS 角色通过映射系 ssertion Marku							
5(应用)之间							

#### 单点登录配置·最佳实践

应用身份服务
--------

添加应用(SAML)	添加SigningKey		$\times$
导入SigningKey 添加	* 名称	cn	
别名	部门名称	请输入部门名称	
	公司名称	请输入公司名称	
	* 国家	CN	~
	* 省份	beijing	
	城市	清癒入城市	
	* 证书长度	1024	~
	* 有效期	180天	~
		<b>提交</b> 取消	

### 3. 导出SigningKey文件

								<u>e</u>
	添加反	应用(SAML)						×
	导出SigningKey	×						
	可以用不同的文件格式导出 SigningKey,在需要单点受书。	援助应用中进行导入该证	度列号	有效期	秘钥算法	算法长度	操作	
要使用的应用进行 1应用,在这里可	DER 编码二进制 X.509(.CER)(D)		1687871404716288794	180	RSA	1024	选择 导	#
	● Base64 编码 X.509(.CER)(S)							
标签		<b>确定</b> 取消						
SSO, SAML,	,阿里云 基于 SAML 协议,实现由 IDaaS 户通过映射实现单点登录到RAM。							
SSO, SAML,	,阿里云 基于 SAML 协议,实现由 IDaaS IDaaS账户和RAM角色通过缺封							
	SAML (Security Assertion Marka							

#### 采用文本编辑器打开,获取到—-BEGIN CERT IFICATE—-—-END CERT IFICATE—-证书信息。 后面操作将用 到该值

8c35041e54954eec8d549098d8817139WYuHfSskQ9Y - 写字板

查看				
$\begin{array}{c c} \hline \\ \hline $	:# # E · # · ■ = = = =	図片         会         日期         插入           図         図         和时间         対象	▲ 查找 ab 替换 ● 全选	
字体	段落	插入	编辑	
	3 • • • 2 • • • 1	BEGIN CERTIFIC, BGINVBAgTAJEyMQswCQYI CZAJBgNVBAYTALNOMQsw gY0AMIGJAoGBAKT8r2vy pqV0E4UQ780SR/X/x/1 qJXbGxXsfWEQhL3ec5QF kkVteDuZQuA9IT+YRJ4C ZCdAIZ9YUSSRhyBaMOBo TBs/C7s= END CERTIFICATI	4 - 1 - 5 - ATE IcNxoU+yK VVQQDewIx CQYDVQQI b1+XUbsOK :SmVgMqd5 :SV7oeH0E Ci7tPy83I i23kLufU4 E	LTOwDQYJKoZIhvcNAQEFBQAwJzELMAkGA1UEBhMCQO4xCzAJ MjAeFwOyMDA4MTQwMJU2MzBaFwOyMDA5MTMwMJU2MzBaMCcx EwIxMjELMAkGA1UEAxMCMTIwgZ8wDQYJKoZIhvcNAQEBBQAD /dtma2vN1u4M6ppUMhO0hsFoVcw3cHSmwbmathOJsDxtB2p0 wWIdkSoYtOqtBKigDetkhOrym38n9okYDHTOBpiRHbZ8P2Br meJPAgMBAEbWQYJKoZIhvcNAQEFBQADgYEAk9dzsQ5NJf17 Nt+Zbkbck79A6qVmBMgZ4+fuh/aDWQQaJALRG4neBrR+8 6D8d22wgvf0+UtDP9jGTVumUF/zbcHcm.covctVeTCCJ=

#### 4. JIRA/Confluence页面配置

#### 访问系统

<u>.</u>	雯索 Q	<del>5</del> 1	<b>?</b> -	¢٠	- 1
更多▼ Q, 高级		JIRA管理 应用程序 项目 问题	5		导出
		酒件 用户管理 最新升级 系统	服告		
根据当前搜索条件没有查询到问题 尝试修改您的搜索条件或者提交一个新的问题	_				

访问插件页面,安装miniOrange Single Sign On插件, 该插件需要付费购买,是JIRA/Confluence 标准单点 登录插件。



访问miniOrange Single Sign On插件 配置页面,参数全部默认生成,只需要调整SP Base URL和SP Entity ID, 填JIRA/Confluence的访问地址

Step 1: Select your Identity	Provider from the following list to see its set	tup guide:				
ADFS	▼ View the Guide					
Your IdP is not in the list? Contac	us using the support/Feedback widget or write to us	at info@xecurify.com and we will help you set it up very quickly.				
Provide this metadata to your Ide	tity Provider to enable JIRA as a service provider/relyi /servlet/saml/metadata Download Metadata C	ng party: Lustomize Metadata				
Use these values below to add JI	RA as service provider/relying party in your Identity Pro	wider:				
SP Entity ID / Issuer		http://123.11 46.33:8080	Сору			
ACSURL		http://1 🖬 💸 46.33:8080/plugins/servlet/saml/auth	Сору			
Single Logout URL		http:// 🙀 🙀 46.33:8080/plugins/servlet/saml/logout	Сору			
Audience URI		http://101000000000000000000000000000000000	Сору			
Recipient URL		http://1335646.33:8080/plugins/servlet/saml/auth	Сору			
Destination URL		http://12212 46.33:8080/plugins/servlet/saml/auth	Сору			
Certificate		Download Show Certificate Details Note: If the IdP requires signed requests, the IdP will need this certificate to validate requests. It is also used to decrypt encrypted SAML Assertions from the IdP. After download, open in notepad to copy certificate. You can configure your own certificates from here.	Сору			
Configure Service Provider	URLs (Optional)					
SP Base I	IRL:* http://:2005.46.33:8080 If your site is behind a proxy you can modify SP Base U	RL for Single Sign-On to work.				
SP Entit	/ ID.* http://*****.46.33:8080 Set the Entity ID for the Service Provider. If not provided Save	I, JIRA base URL will be used by default.				
step 2: Import IdP Metadata or note down the following information from your IdP and keep it handy. Click the next button below when you are ready. 刀换第二个页面, Configure IDP页面						

ervice Provider Info	User Profile User Groups SSO Settings Certificates Backup/Restore Configurations User Directory Info
Manual Configuration Impo	rt From Metadata
Add Identity Provider	
Step 3: Configure IDP	
Click on Import From Metadata to fe	tch IDP's settings from IDP metadata URL or XML file OR copy the URLs from Step 2 below to setup IDP details.
Need help with the configuration? Co	ntact us using the support/Feedback widget or write to us at info@xecurify.com and we will help you set it up very quickly.
IDP Name	La DaaS
	This IDP Name will be shown in the login widget to users.
IDP Entity ID / Issue	T IDaaS
	Enter the Entity ID or Issuer value of your Identity Provider. You can find its value in the entityID attribute of EntityDescriptor tag in IdP-Metadata XML file.
Send Signed Requests	It is recommended to keep it checked. Uncheck, only if your IdP is not accepting Signed SAML Request.
SSO Binding Type	◎ Use HTTP-Redirect Binding for SSO ◎ Use HTTP-Post Binding for SSO
Single Sign On URL	* https://fwsgggaypr.login.aliyunidaas.com/enduser/bff/sso/go_6fc79af807581d5t
	Enter the Single Sign-on Service endpoint of your Identity Provider. You can find its value in SingleSignOnService tag (Binding type: HTTP-Redirect) in IdP-Metadata XI
SLO Binding Type	$\odot$ Use HTTP-Redirect Binding for SLO $\odot$ Use HTTP-Post Binding for SLO
Single Logout URL	<u>.</u>
	Enter the Single Logout Service endpoint of your Identity Provider. You can find its value in SingleLogoutService tag in IdP-Metadata XML file. Leave blank if SLO not s
NameID Forma	Urn pasis names to SAME 2 0 nameld format persistent
Hameld Forma	Select the name identifier format supported by the IdP.Select unspecified by default.

#### 参数说明

- IDP Name: 可以随意填写;
- IDP Entity ID/Issuer: 需要和IDaaS的IDaaS IdentityId值一致,建议统一写成: IDaaS;
- Send Signed Requests 需要勾选;
- SSO Binding Type:勾选第一项;
- Single Sign On URL: 填IDaaS的发起地址,下面步骤中将介绍获取方式
- NameID Format: 选择SAML:2.0 nameid-format persistent;(IDaaS应用中需配置一致);
- IDP Signing Certificate: 此处填步骤3中获取的证书信息。
- 5. 返回IDaaS控制台,继续创建SMAL应用

选择SigningKey

	添加应用(SAML)					:	×
	导入SigningKey 添加SigningKe	у					
	别名	序列号	有效期	秘钥算法	算法长度	操作	
要使用的应用进行初始化配置,并开始后续使用。 1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登录3	CN=cn, ST=beljing, C=CN	1687871404716288794	180	RSA	1024	选择导出	
标签 描述							
SSO, SAML, 阿里云 基于 SAML 协议, 实现由 IDaas 户通过映射实现单点整灵到RAM							
SSO, SAML, 阿里云 基于 SAML 协议,实现由 IDaaS IDaaS账户和RAM角色通过映射							
SAML (Security Assertion Mari SSO, SAML (IDaaS)和满數方 (应用)之 常广泛的运用。	9						
WordPress 是全世界最初广泛使 SSO, SAML, CMS 允许千万技术或相技术人员生产 支持通过 SAML 协议单点登录到							
SSO, 用户同步, SAML, 基于 SAML 协议, 实现由 IDaaS							

#### 填写应用信息

	添加应用(SAML)	:
现单点登录功	图标	SAML ②上传文件 图片大小不超过1MB
	应用ID	idaas-cn-hangzhou-zum7yejeis3plugin_saml
	* 应用名称	JIRA
≷现由 IDaaS ◎登录到RAM。	* IDaaS IdentityId	IDaaS IDaaS IdentityId is required
駅由 IDaaS 色通过映射家 sertion Marki	* SP Entity ID	http:// ▮ 👔 📫 .46.33:8080 SP Entity ID is required
(应用) 之间	* SP ACS URL(SSO Location)	http:// 💵 🐭 46.33:8080/plugins/servlet/saml/auth
■最被广泛使用 注 人员生产、 2 单点登录到	SP 登出地址	请输入SP 登出地址
砚由 IDaaS	* NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent ~
	Assertion Attribute	Assertion Attribute key     请选择     -     +       断言属性。设值后,会将值放入SAML断言中。名称为自定义名称,值为账户的属性值。
	Sign Assertion	
	IDaaS发起登录地址	IDaaS <u>发起警录地址</u> 以 http://、https:// 开头, 填写后使用 IDaaS 发起登录将会跳转到该地址, 而不会使用 SAML 的idp发起登录流程
	* 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)

- 应用名称: 可以随意填写;
- IDaaS IdentityId: 建议统一写成: IDaaS;

- SP Entity ID: 填写JIRA/Confluence 基础访问地址
- SP ACS URL(SSO Location): 填写JIRA/Confluence Service Provider Info 页面的ACS URL参数
- NameldFormat: 选择SMAL:2.0 nameid-format persistent
- 选择一种账户关联方式进行提交,应用创建成功

#### 在机构及组页面创建一个IDaaS账户

概览		机构及组								
快速入门										
应用 应用列表 添加应用	^	机构及组 管理员在当前页面对组织架构、部门及其包会的组、账户进行管理,也可以使用AD、LDAP 或 Excel文件的方式配置导入或同步。 在左侧的组织架构树中,可以右键点由某个部门对其进行操作,也可以左键选择某个部门,并在右侧为其进行创建账户、创建组、创建部门等操作。								
账户	^	组织架构 查看详情								
账户管理		在这里对他们能通过了管理。左键可选择组织机 × 账户 组 组织机构								
分类管理		19,41897A3组7004987138679								
认证	^	M 阿里云IDAAS								
认证源		当前账户数 2 / 已购套餐规俗为 100								
RADIUS		编号 账户名称 显示名称 类型 目录								
证书管理										
授权	^	1 2001 2001 回递购一 /								
权限系统		2 idaas_manager 默认管理员 自建账户 /								
应用授权										
审计	~									
其它管理	~									

#### 在应用授权页面,把应用授权给新创建的账户,并保存

概览		应用授权									
快速入门		按应用授权组织机构组 按组织机构/组授权应用 按账户授权应用 按应用授权	以账户 按分类授权应用								
应用	^										
应用列表 添加应用		按账户授权应用 重進为指定账户授权指定应用。	按账户授权应用 直接为指定账户授权指定应用。 用示								
账户 机构及组	^	* 旋水:这里展为的分析不通,预与迷白角果处用化模1,而是,预与迷白直接很权到果处用1。然与网样可以通过具所属组织的内,所属组等黑道或或果处用的化料。 可以通过账户管理查看到某个账户所拥有的全部应用权限信息。									
账户管理 分类管理		账户(2) 应用数 (1) 已授	权(1)个								
认证	^	请输入账户名称进行重线 Q 请输入应用名称进	57.微水								
认证源 RADIUS		zb01 >> 区用部	各称 应用ID								
证书管理		idaas_manager > 🛛 JIRA	idaas-cr	1-hangzhou-ty050sw67fp							
授权 权限系统	^	共2. ( 1 )									
应用授权		保存									
审计	~										
其它管理	~										
设置	~										

#### 访问应用列表,点开应用详情,点击查看应用子账户

T-+ BM TT X14 BUI TO O TO TO TO TO TO

88

#### 单点登录配置·最佳实践

大道入门 立用 应用列表 添加の用	^	应用列表 管理员可以在当能页面管理已 当添加先应用局,应该确认应	经添加的所有应用,应用可以实现单点叠接和数据 用处于后用状态,并已经完成了接权。在应用详情	啊步能力。 中,可以看到应用的详细信息、单点登	录地址、子乐户配置、同步配	重、授权、审计等信息。			
K户	^	请输入应用名称			٩				
机构及组		应用题标 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		JIRA	idaas-o	cn-hangzhou-zum7yejeis3plugin_saml	Web <u>应</u> 用		$\checkmark$		授权 详情 ▲
从正	^								
认证源 RADIUS		应用信息	认证信	1.0		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	9单点登录地址		SCIM协议设置以及把组织机构、组同	步推送至应用	平台主账户与应用系统中子账户	的关联表
受权 权限系统	^	查看详情 修改应用 删除	e应用 IDeaS	8发起地址		同步机构 SCIM配置		查看应用子账户	
应用授权		授权信息	审计信	也		API		管理应用内权限	
₩17 展它管理 <sup>●</sup>	Ĵ	应用与人员组织的授权关系	立香壺	包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	
日間	~	授权	查看日	日志 查看同步记录		API Key API Se	cret	鄉定权限系统	

#### 添加账户关联

#### 主账户: IDaaS中的账户, 上面在账户及组页面创建的账户

子账户: JIRA/Confluence 中的账户, 如登录JIRA/Confluence账户名是admin, 子账户填写admin

应用列表 / 子账	<del>ا</del> ر:									
← 子账户	・子账户									
子账户 デ账户: 学例: 账户关	子報中     子報中     子雅の指始後是石指定迎用系統中,用户会以什么身份进行访问。主称の指的是 (DaaS 中的原本,在进行单位整要时, IDaaS 会向应用系统传播对应的子预产,该子预产需要在应用系统中存在目前问题。     学校:「DaaS 中容主矩户 弦三 (用户名 changiam), 正全社的 BPM 通用系系中,这个用户的用户名量 apoodman, 影子频产力法mytam 进行关系,     斯户关联方式,在应用领理时,如果选择了资产冲换时,回题以主联户位子指小的学校中全全。无案能量、如果选择了货产人类和,需要要任企型进行手动的子预产创建和主子标户处理。									
JIRA										
主账户 (账户名	称)			٩						
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			
zb01	zb01	admin	无	已关联	无	2020-08-14	删除			
	_					共 1	条 < 1 > 跳至	1 页		

返回应用详情,复制 IDaaS发起地址, 粘贴到JIRA/Confluence的 Configure IDP页面Single Sign On URL 参数中,并进行保存。

······ 快速入门 应用 ^		应用列表 管理员可以在当前页面管 当场10亩应用后 应该输	理已经添加的所有应用,应用可以实现单点 以立用外干完用化本,并已经需求了提供了	登录和数据网络能力。 在应用注标中 可以类别应用	的迷想痛苦 单点酸恶物碱 子导	白野香 同步群	8 1847 (19)十95/418			
添加应用 账户 ^	请给	111040427432713187,2216644 入应用名称	WOZYDAL J INIYOVAN YY LABEYDAU J ISOA		nanuwaliker ↔warnever a v	Q	an index and an index			
机构及组	应用	國标 应用名称		应用ID		设备类型		应用状态	二次认证状态	操作
分與管理	5	JIRA		idaas-cn-hangzhou-zum	7yejeis3plugin_saml	Web应用		$\checkmark$	×	授权 详備 🔺
认证 ^										
认证源 RADIUS		应用信息		认证细胞			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	推送至应用	平台主账户与应用系统中子账户	的关联表
授权 个		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	
权限系统 应用操权										
214		授权信息		审计信息			API		管理应用内权限	
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	旧志		是否对应用开放系统API		管理应用内菜单与功能权限	
没置 ~		授权		查看日志 查看同時	紀景		API Key API Sec	et	绑定权限系统	

Service Provider Info Config	ure IDP User Profile User Groups SSO Settings Certificates Backup/Restore Configurations User Directory Info
Manual Configuration	n Import From Metadata
Add Identity Provider	
Step 3: Configure IDI	
Click on Import From Met	adata to fetch IDP's settings from IDP metadata URL or XML file OR copy the URLs from Step 2 below to setup IDP details.
Need help with the configu	ration? Contact us using the support/Feedback widget or write to us at info@xecurify.com and we will help you set it up very quickly.
	IDP Name. IDaaS
	This IDP Name will be shown in the login widget to users.
IDP Entity	ID / Issuer.* IDaaS
	Enter the Entity ID or Issuer value of your Identity Provider. You can find its value in the entityID attribute of EntityDescriptor tag in IdP-Metadata XML file.
Send Signer	I Requests: It is recommended to keep it checked. Uncheck, only if your IdP is not accepting Signed SAML Request.
SSO Bi	nding Type:
Single Si	n On URL:* https://fwsgggaypr.login.aliyunidaas.com/enduser/bff/sso/go_6fc79af807581d5
	Enter the Single Sign-on Service endpoint of your Identity Provider. You can find its value in SingleSignOnService tag (Binding type: HTTP-Redirect) in IdP-Metadata XML
SLO Bi	nding Type:
Single I	
oligie 2	Enter the Single Logout Service endpoint of your identity Provider. You can find its value in SingleLogoutService tag in IdP-Metadata XML file. Leave blank if SLO not sup
Nam	eID Format: urn:oasis:names.tc:SAML:2.0:nameid-format:persistent
	Select the name identifier format supported by the IdP.Select unspecified by default.

#### 6. 单点登录JIRA/Confluence

#### 访问IDaaS 用户登录地址

实例列表									
实例ID/名称	标准版实例ID	状态 (全部) ∨	规格授权	最大用户数	到期时间	产品版本	用户登录页地址	实例开放接口域名	操作
idaas-cn-hangzhou-y 081 (va 71):	idaas-cn-st27; 🏣 ҧ 🗇	运行中	增强版	100	2020年9月15日	V1.7.7	for the login aligunidaes.com	î <b>⊪¶,, p</b> r⊣pi.aliyunidaas.com	管理 升级 续费
								く上一页 1	下一页 >

#### 输入上文中创建的IDaaS账户进行登录

简体中文	扫码登录更便捷		1
	D		
ß0]≚	里云IDAAS		
zb01		-	
•••••			
DCM0			
	忘记密码		V
	提交		
	简体中文 [2b01 [DCM0]	資体中文       日田登录更便想         「「日田登录更便想         「「日田登录更便想         「「日田登录更便想         「「日田登录更便想         「「日田登示更便想         「「日田登示更便想         「「日田登示更優遇         「日田登示	商休中文 の の の の の の の の の の の

#### 点击应用图标进行单点登录

IDaaS统—认证与	影份半台	
欢迎 · IDaaS		我的应用
主导航	^	Web应用
首贞		
应用管理		
应用子账户		SAME
设置	^	
我的账户		JIRA
二次认证		
我的消息		
我的日志		移动应用
		当前没有接权的移动应用。
	X次迎・IDaaS     文     文     文     プ     ジ	DaaSS     、     、     、     、     、     、     、     、     、     、     、     、     、     、     、     、     の用管理     应用予账     、     の用でいた     、      、

### FAQ

#### IDaaS是否支持同步数据到JIRA/Confluence

IDaaS不支持直接和JIRA, Confluence 进行数据同步,因为JIRA, Confluence是标准产品不支持改造,只能适应JIRA, Confluence支持的LDAP同步方式。建议同步流程: IDaaS账户数据变动可以同步到LDAP, JIRA, Confluence 再拉取LDAP中的账户变动信息实现同步。IDaaS同步数据到LDAP,请参考LDAP账户同步配置。

## 1.4. JIRA对接-使用SSO 2.0

本文为您介绍如何通过Jira的SSO 2.0配置单点登录。

### 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. 在左侧导航栏,点击 应用 > 添加应用,选择SAML应用模板,点击添加应用。

快速入门		全部 标准协议	定制模板					
应用 应用列表 添加应用 账 <sup>声</sup>	^	添加应	用 8合了所有已支持的可添加应 5两种:一种是支持标准的 JV	用列表,管理员可以选择需要 VT、CAS、SAML 够模板的5	使用的应用进行初始化配置。 应用,在这里可以通过添加对	并开始监修数据。 如外游动范围教室来采取单点重要功能,另一种重量制应用,本舆应用已经提供了对接取单点重要成用小用计划接口,由 IOwad 为和我的注意化线索因	行对接。	×
机构及组 账户管理		SAML				- Q		
分與管理		应用图标	应用名称	应用ID	标签	描述	应用类型	操作
い证 い证瞭	^	<b>C</b> -J	阿里云RAM-用户SSO	plugin_aliyun	SSO, SAML, 阿里云	基于 SAML协议,实现由IDa85单点撤录到周围云控制台;使用床模板,需要在RAM中方向个用户单级创建RAM子张户,IDa85账户fDRAM子账 户者过8955实现单点型使到RAM。	Web应用	添加应用
RADIUS 证书管理		<b>C</b> -J	阿里云RAM-用户SSO	plugin_aliyun_role	SSO, SAML, 阿里云	基于 SAML协议,实现由 (DaaS 单点量量到同量完结构);使用床模拟,需要RAM中创建RAM角色,不需要为每个用户单绘创建RAM子核户, [DaaS核产和RAM角色通过接到东京制作点型录到RAM,	Web应用	添加应用
授权 权限系统	^	S	SAML	plugin_saml	SSO, SAML	SAML (Security Assertion Markup Language, 安全新宣布记录图, 版本 20) 基于 XML 协议,使用组合等部(Assertion)的安全今律,在现分方 (Doase) 和高振方(应用)之间地递身份信息,实现基于网络阿姆的单项塑像。SAML 协议是成款的认证协议,在现内外的公务会行和指表于中有非 常广泛投资用。	Web应用	添加应用
应用援权 審社	~		WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress 是全世界最近了还有的 CMS(Content Management System,内容理理系统),立地过去将强化均衡并最终能力便回路的进行界流 允许不万股水或印技术人员生产,管理是特殊型的问题。从肯定问题。政府问题到个人培客,主题论坛、WordPress 所交地的历纪年常多样。IDaaS 艾特通过 SAML 的汉集中登录员 WordPress 问题。	Web应用	添加应用
其它管理	~	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 到阿爾納德的单点邀集和用户同步。	Web应用	添加应用
化量	Ŷ					共5条	< 1 → 10 剱页 >	

#### 添加SigningKey

	添加应用(SAML)							×
	导入SigningKey	添加SigningKey						
	别名	序列号		有效期	秘钥算法	算法长度	操作	
现单点登录功			暂无数据					
实现由 IDaaS 点登录到RAM。								
实现由 IDaaS 争色通过映射系 ssertion Marki								

#### 单点登录配置·最佳实践

添加应用(SAML)	添加SigningKey		$\times$
导入SigningKey 添加	* 名称	cn	
别名	部门名称	请输入部门名称	
	公司名称	请输入公司名称	
	* 国家	CN	~
	* 省份	beijing	
	城市	请输入城市	
	* 证书长度	1024	~
	* 有效期	180天	~
		提交取消	

#### 3. 导出SigningKey文件

								<u>e</u>
		添加应用(SAML)						×
	导出SigningKey	×						
	可以用不同的文件格式导出 SigningKey,在需要书。	单点登录的应用中进行导入该证	序列号	有效期	秘钥算法	算法长度	操作	
要使用的应用进行 1应用,在这里可	○ DER 编码二进制 X.509(.CER)(D)		1687871404716288794	180	RSA	1024	选择 导:	±
	◉ Base64 编码 X.509(.CER)(S)							
标签		确定取消						
SSO, SAML	,阿里云 基于 SAML 协议,实现由 IDaaS 户通过缺射实现单点登录到RAM。							
SSO, SAML	,阿里云 基于 SAML 协议,实现由 IDaaS IDaaS账户和RAM角色通过缺时							
	SAML (Security Assertion Mark							

采用文本编辑器打开,获取到—-BEGIN CERT IFICATE—-—-END CERT IFICATE—-证书信息。 后面操作将用 到该值

8c35041e54954eec8d549098d8817 查看	'139WYuHfSskQ9Y - 특	字板		
$\frac{11}{2} \cdot \mathbf{A}^* \mathbf{A}^*$		■ ジジ ■ ↓ 図片 绘 日期 插入 ・ 図 和时间 对象	<ul> <li>▲ 査找</li> <li>♣ 査找</li> <li>♣ 査扱</li> <li>● 全选</li> </ul>	
	3 + 1 + 2 + 1 + 1	BEGIN CERTIFIC, BEGIN CERTIFIC, BONDAGTA, BEMQSwCQYI CzAJBgNVBAYTAKNOMQsw gYOAMIGJAGBAKt8r2yc pQVOE4IQ780SR/X/x/11 qJXbGxXsfWEQhk3ec5QF kkVteDu2QuA91T+YRJ4C ZCdAIz9YUSSRhyBaMOBC TBs/C7s= END CERTIFICAT	ATE IcNxoU+yK VQQDEwIx vCQYDVQQI 51+XUbsOK tSmVgMqd3 7sV7oeHOE Ci7tPy831 j23kLufU4 E	LTowDQYJKoZIhvcNAQEFBQAwJzELMAkGA1UEBhMCQO4xCzAJ MjAeFwOyMDA4MTQwMjU2MzBaFwOyMDA5MTMwMjU2MzBaMCcx EwIxMjELMAkGA1UEAxMCMTIwg2SwDQYJKoZIhvcNAQEBBQAD /qHma2vN1u4M6ppUMh00h5FoVcw3cHSmwbmath0J5DxtB2p0 wWIdkSoYtOqtBKigDetkhOrym38n9okVDHTOBpiRHbZ8P2BR meJPAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAk9dzsQ5NJf17 Nt+Zbkbck79A6qVmBMg24+fuh/apMQQaJoLRLG4neBrR4+8 6D8d22wgvf0+UtDP9jGTVumUF/

#### 4. JIRA页面配置

访问system

Q Search	🔶 😚 🔶
	JIRA ADMINISTRATION
	Applications
	Projects
	Issues
	Manage apps
	User management
	Latest upgrade report
	System

选择SSO 2.0

Applications Projects Issues	Manage apps User management Latest upgrade report System
General configuration Find more admin tools Jira mobile app SYSTEM SUPPORT System info Instrumentation JMX Monitoring	Configure how users log in Authentication method SAML single sign-on Users log in using a SAML Identity Provider. SAML SSO 2.0 settings Single sign-on issuer*
Database monitoring	IDaaS
Integrity checker	The entity ID from your provider, e.g https://www.example.com/ab123
Logging and profiling	Identity provider single sign-on URL.*
Scheduler details	https://t.1-ikg-c.es.login.aliyunidaas.com/enduser/api/application/plugin_saml
Troubleshooting and support tools	The SAML 2.0 SSO URL from your provider. e.g. https://www.example.com/abc123/sso
Audit log	X.509 Certificate*
Clustering SECURITY Project roles Global permissions	BEGIN CERTIFICATE IMBEGIN CERTIFICATE GATUEBhMCQ04xCZAJ BgNVBagTAjEyMQswCQYDVQQDEwixMjAeFw0yMDA4MzEwNzU0MzdaFw0 yMDA5MzawNzU0MzdaMCcx CzAJBgNVBAYTAKNOMQswCQYDVQQIEwixMjELMAkGATUEAxMCMTiwgZ8
Password Policy	Copy and paste the entire X.509 certificate that you got from your provider.
User sessions	Username manning *
SSO 2.0 Remember my login Whitelist	S(NameID) Used to map IdP attributes to the username, e.g. \$(NameID)
Issue collectors	Give these URLs to your identity provider Assertion Consumer Service URL

#### 参数说明

- Authentication method:选择SAML single sign-on
- Single sign-on issuer: 建议统一写成 IDaaS
- X.509 Certificate:此处填步骤3中获取的证书信息。
- Identity provider single sign-on URL:格式为 https://xxxxxx.login.aliyunidaas.com/enduser/api/application/plugin\_saml/idaas-cn-shanghaixxxxxx/sp\_sso

#### https://xxxxxx.login.aliyunidaas.com获取方式查看下图

华东	2(上海) 🔻				Q 搜索文档、	控制台、API、解决方案	和资源 费	用 工単 备案	企业	支持
	实例列表									
	实例ID/名称	标准版实例ID	状态 (全部) 🗸	规格授权	最大用户数	到期时间	产品版本	用户登录页地址		
	idaas-cn-shanghai-in 👫 👘 🗤	idaas-cn-9a1vtva 🗊 🗇	运行中	增强版	100	2020年11月24日	V1.7.7	📫 her opg. login.al	yunidaas.c	om

idaas-cn-shanghai-xxxxx获取方式查看下图

#### 应用身份服务

■ (-)阿里云				Q 搜索文档、 控	制台、API、解决方案和资源	费用 工単	备案	企业	支持	官网	>_
概览		应用列表		应用详情 (SAML)							
快速入门											
应用 ^ <u> 应用列表</u> 添加应用	I	应用列表 管理员可以在当前页面管理已经添加的所 当添加完应用后,应该确认应用处于自用	有应用,应用可以实现 <b>单点登录和数据同</b> 步能力。 肤态,并已经完成了接段。在应用详情中,可以看到应用的详细信息、单	图标	SAML						
彩白 ~				应用ID	idaas-cn-shanghai-lu <b>t 1 , (m</b> . Of	saml2					
机构及组		应用图标 应用名称	成用ID	应用名称	SAML						
分类管理		SAML	idaas-cn-shanghai-hy	CippingKau	126962802280 BE 0/(0)-12	, ,					
认证 ^				SigningKey	130002032220131#000(CIV-12)	)					
RADIUS		应用信息	认证信息	NameldFormat	urn:oasis:names:tc:SAML:2.0:na	ameid-format:per	sistent				
证书管理		应用的详细信息	应用的单点登录地址	SP ACS URL	https://www.www.https://plugins/s	ervlet/samlconsu	imer				
授权 へ 权限系统		查看详情修改应用删除应用	IDaaS发起地址	IDaaS IdentityId	IDaaS 导出 IDaaS SAML 元配雪	这件					

5. 返回IDaaS控制台,继续创建SMAL应用

#### 选择SigningKey

		添加应用(SAML)					×
		导入SigningKey 漆	∭SigningKey				
		别名	序列号	有效期	秘钥算法	算法长度	操作
要使用的应用进行初始化配置, 1应用,在这里可以通过添加对	,并开始后续使用。 应的标准应用模板来实现单点登录功	CN=cn, ST=beijing, C=CN	1687871404716288794	180	RSA	1024	选择导出
标签	描述						
SSO, SAML, 阿里云	基于 SAML 协议,实现由 IDaaS 户通过映射实现单点登录到RAM,						
SSO, SAML, 阿里云	基于 SAML 协议,实现由 IDaaS IDaaS账户和RAM角色通过映射到						
SSO, SAML	SAML(Security Assertion Marko (IDaaS)和消费方(应用)之间 常广泛的运用。						
SSO, SAML, CMS	WordPress 是全世界最被广泛使/ 允许千万技术或非技术人员生产。 支持通过 SAML 协议单点登录到						
SSO, 用户同步, SAML,	基于 SAML 协议,实现由 IDaaS						

填写应用信息

	④上传文件 图片大小不超过1MB
应用ID	idaas-cn-shanghai-hx5.0000 multic phogin_saml2
* 应用名称	SAML
* IDaaS IdentityId	IDaaS IDaaS Identituld is required
* SP Entity ID	https://
	SP Entity ID is required
* SP ACS URL(SSO Location)	https://jira.chad.el.a
SP 登出地址	请输入SP 登出地址
* NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
Assertion Attribute	NameID
	断言属性。设值后,会将值放入SAML断言中。名称为自定义名称,值为账户的属性值。
Sign Assertion	
IDaaS发起登录地址	IDaaS发起登录地址
	以 http://、https:// 开头, 填写后使用 IDaaS 发起登录将会跳转到该地址, 而不会使用 SAML 的idp发起登录流程
*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)

- 应用名称: 请填写一个应用名称;
- IDaaS IdentityId: 建议统一写成 IDaaS;
- SP Entity ID: 填写JIRA中的Audience URL (Entity ID), 见下图
- SP ACS URL(SSO Location): 填写Jira中的Assertion Consumer Service URL,见下图
- NameldFormat: 选择SMAL:2.0 nameid-format persistent
- Assertion Attribute: 输入NameID, 选择应用子账户
- 开启Sign Assertion
- 选择一种账户关联方式进行提交,应用创建成功
#### 应用身份服务

User sessions						
SSO 2.0	Username mapping					
Remember my login	\${NameID}					
Whitelist	Used to map IdP attributes to the username, e.g. \${NameID}					
	Give these URLs to your identity provider					
issue collectors	Assertion Consumer Service URL					
USER INTERFACE	https://j.m.downed.com/ploging/domiet/somiconsumer					
Default user preferences						
System dashboard	Audience URL (Entity ID)					
Look and feel	https://ji ••• in leta.org					
Announcement banner						
Rich text editor	JIT provisioning Just-in-time user provisioning allows users to be created and updated automatically when they log in through SSO to Atlassian Data Center applications. Learn m	iore.				
IMPORT AND EXPORT	Create users on login to the application					
Backup system						
Restore system	SAML SSO 2.0 behaviour					
Project import	Remember user logins					
External System Import	Save successful login history and log in users automatically without the need for reauthentication.					
	Login mode*					
MAIL	<ul> <li>Use SAML as secondary authentication</li> </ul>					
Outgoing Mail	Users will log in using a login form by default, they can log in using single sign-on through the identity provider or by using this link.					
Incoming Mail	<ul> <li>Use CAML as primary authention.</li> </ul>					
Mail queue	Use SAML as primary authentication Redirect browser-based users to the IDP when they visit the in-ann login form. REST and other requests are still					
Send email	permitted. Learn more.					
Batching email notifications						

#### 在机构及组页面创建一个IDaaS账户



在应用授权页面,把应用授权给新创建的账户,并保存

#### 单点登录配置·最佳实践

概览		应用授权		
快速入门		按应用授权组织机构/组 按组织机构/组授权应用 按账户授权	<u>应用</u> 按应用授权账户 按分类授权应用	
应用 应用列表 添加应用 账户 机构及组	^	按账户授权应用 重接为据定应用。 提示:这里账户的并不是「账号是否有某应用权限」,而是   可以通过账户管理查看到某个账户所拥有的全部应用权限信息	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。 。	
账户管理 分类管理		账户(2)	应用数 (1) 己振识(1)个	
认证 认证源 RADIUS	^	请输入账户省积进行查线         Q           zb01         >	請給入应用≤称进行撤末 ☑ 応用名称	应用ID
证书管理		idaas_manager >	🔸 🗹 JIRA	idaas-cn-hangzhou-ty050sw67fp
授权 权限系统 应用授权	^	共2条 〈 1 〉		
审计	~		<b>保存</b>	
其它管理	~			
设置	~			

#### 访问应用列表,点开应用详情,点击查看应用子账户

央道入门								
应用 应用列表 添加成用	^	血用列表 留理則可以在当該共應管理已起活成的所有应用,应用可以实現學血發展低數類同時能力, 当該或加加包用品,应该與人应用於于面积状态,并已過來用或了個代,在应用非幾中,可以靠到应用的中間信息,单心發展地址,子聚介配置,因於配置,時化,面计都信息,						
版户	~	请编入应用名称		Q				
机构及组 账户管理		应用器标 应用名称	应用ID	设备类型	应用状态	二次认证状	き 操作	
分类管理		JIRA	idaas-cn-hangzhou-zum7yejeis3plugin_saml	Web应用	$\checkmark \bigcirc$	×	授权 详情 🔺	
大正	^							
认证原 RADIUS		应用信息	认证信息		账户信息 - 同步	账户信	直 - 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、组同步推送至应用	平台主	账户与应用系统中子账户的关联表	
受权 权限系统	^	<b>查看洋情</b> 停改应用 删除应用	IDaaS波起地址		同步机构 SCIM配置	查看点	7用子账户	
应用授权								
R3+		授权信息	审计提思		API	管理应	用内权限	
展它管理	÷	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	管理点	7用内菜单与功能权限	
2重	~	援权	查看日志 查看同步记录		API Key API Secret	課定も	初聚系统	

#### 添加账户关联

#### 主账户: IDaaS中的账户, 上面在账户及组页面创建的账户

子账户: JIRA 中的账户, 如登录JIRA账户名是admin, 子账户填写admin

				G. 2000000 200	BELO SERVICES	Tt 1% TT X14 10	
· 列表 / 子账户							
子账户							秦加账户关联 批量导入 ;
子報户 ◇							
RA							
主账户 (账户名称)				Q			
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
zb01	zb01	admin	无	已关联	无	2020-08-14	删除
						共1条	〈 1 〉 跳至 1

#### 6. 单点登录JIRA

#### 复制jira中的link地址进行访问

Announcement banner Rich text editor	<b>JIT provisioning</b> Just-in-time user provisioning allows users to be created and updated automatically when they log in through SSO to Atlassian Data G				
IMPORT AND EXPORT	Create users on login to the application				
Backup system					
Restore system	SAML SSO 2.0 behaviour				
Project import	Remember user logins				
External System Import	Save successful login history and log in users automatically without the need for reauthentication.				
	Login mode*				
MAIL	<ul> <li>Use SAML as secondary authentication</li> </ul>				
Outgoing Mail	Users will log in using a login form by default, they can log in using single sign-on through the identity provider or by				
Incoming Mail	using <u>this link</u> .				
	<ul> <li>Use SAML as primary authentication</li> </ul>				
Mail queue	Redirect prowser-based users to the IDP when they visit the in-app login form. REST and other requests are still				
Send email	permitted. Learn more.				
Batching email notifications					
▶ https://j=n.cland=taid=g/plug	gins/servlet/external-login				

#### 输入上文中创建的IDaaS账户进行登录,登录成功后直接访问到Jira。

简体中文	扫码登录更便捷	
	D	
问旦 zb01	본조IDAAS	•
•••••		
DCM0		
	忘记密码	

### FAQ

是否支持通过IDaaS门户单点登录到Jira。

IDaaS统—认证身份平台			
欢迎 · IDaaS	我的应用		
王导航 ^	Web应用		
应用管理			
应用子账户	S		<b>C</b> -7
设置 ^	SAML	JWT	
我的账户	SAML	JWT-1103	阿里云RAM-用户SSO
二次认证		未添加账户	未添加账户
我的消息			
我的日志	移动应用		

支持。具体信息请查看Jira/Confluence对接。

# 1.5. SAP GUI对接

本文为您介绍如何配置实现SAP GUI的单点登录

### 操作步骤

1. 在SAP客户端添加新条目

#### 创建新系统条目

>

选择连接类型并按要求更改系统参数。 如果想让系统建议描述,则保留描述字段为空。 输入所有必需的数据 后,按钮"下一步(N) >"和"完成(F)"方才激活。

连接类型:	自定义应用程序服务器	~
系统连接参数		
描述:	<u>[</u> ]	
应用服务器:	-	
实例编号:		
系统标识:		
SAProuter 字符串:		

□ 使用此页面作为后续条目创建的首页; 设置立即生效

帮助( <u>H</u> )	取消( <u>C</u> )	〈上→步(B)	下一步(N) >	完成(E)

应用服务器,实例编号,系统标识由客户提供。服务器版本: S/4 HANA 1610

2. 登录SAP

=		<	6	_ [	
SAP		SAP			
~	新密码 更多 >				ш
集团:		信息			
		☑ 欢迎使用S/4云端测试系统			
*用户:		S/4 1610 SP05(2019/11)			
*密码:	*****	CLIENT700 正常运行			
称录语言。	7H	■ CLIENT800 , 来源于client	700, 20	019.12.	09
. 自印水.近	211				

输入用户名密码进行登录。

3. 添加证书 左上角输入 STRUSTSSO2 回车

≡						
SAP						
STRUSTSS02	✓ SAP 菜单	SAP 业务工作台	其它菜单	添加到收藏夹	创建角色	更多、
□ 收藏夹						
◇ ① SAP 采単 > □ Financial Service	s Network Conne	ector				
> □ 办公室						
>□交叉应用组件 >□方后勤						
> □ 会计核算						
>□人力资源						
>口日忌永坑						
> 🗋 WebClient 用户界面	面框架					

< SAP			
✓ 显示 <-> 頁	更改 更多 ~		
>□系统个人安全环境	系统个人安全环境		
> □ SSL 服务器 标准	自己的证书		
> □ SSL 客户端 SSL 客户端(匿名) > □ SSL 客户端 SSL 客户端(标准)		主题:	CN=SYS, OU=SAP Test, O=mySAP.com Workpl
> ] Web 服务安全性 标准			(自签名)
→ Web 服务安全性 Web 服务安全性键值			颁发者证书
⊗ SMIME 标准			
◎ 又针 > □ 安全存储和转发 协作集成库: oAuth			
> □ 安全存储和转发 在线学习			
> □ 安全存储和转发 FI_MAP ⑤ 安全存储和转发 登录更证			
> □ 安全存储和转发 ZMYAPP			信任师告来证书
			口TL/灰人有 llL 17

#### 依次点击 "显示 ↔ 更改" → "更多" → "个人安全环境" → "导入",选择system.pse 文件,完成 后如图所示

		使用登录票证的单点登录的信任管理器; 更改	
> 第章 ↔ 東	改 更多~		Exit
系统个人安全环境 SNC SLP 来到库	文件		
155L 服务器 标准 155L 客户端 55L 客户端 (Ⅲ名)	自己的证书		
\$51. 客户塔 \$51. 客户塔(标准) Web 服务安全性 标准	10 11	(高等点)	
Web 服务安全性 其他系统加密证书 Web 服务安全性 Web 服务安全性智值 SMINE 标准		<b>建发表证书</b>	
alle Peter 文作 安全存储和转发 转作集成库; oAuth 安全存储和转发 在线学习 安全存储和转发 F1_MAP			
安全存储和转发 登录票证 安全存储和转发 DIGAPP		- 你在感觉者近年	
	证书列表		
		18	
	Θ		
		a 1961	
	土 职业个人买至环境	8 mm	

双击证书列表中 "CN=mySAP.com Workplace CA (dsa), O=mySAP.com Workplace, C=DE",证书列表 中证书将会在证书栏显示详细信息

=				< 60 _ 67 ×
< SAP		使用登录票证金	的单点登录的信任管理器; 更改	
♥ 勘定 (つ )	更改 更多 🗸			Exit
> □ 長焼个人交全外残 > □ 気焼个人交全外残 □ 502 54P 室円序 > □ 502 54P 室円序 > □ 502 57P 索 501 57P 南(田名) > □ 503 57P 南 501 57P 南(田名) > □ 540 服务交全社 系印南(田名) > □ 540 服务交全社 其他系统如新证书 > □ 540 服务交全社 核由 服务交全社経費 @ 3000 医水液 @ 32月 > □ 540 欠約和約2 物点性理形。aboth	证书列表	1.8		
<ul> <li>□ 支全庁協和特徴 (東京)</li> <li>○ 支全庁協和特发 (FL) SAP</li> <li>□ 支全庁協和特发 (L) 表示</li> <li>□ 支全庁協和特发 (L) 表示</li> <li>□ 支全庁協和特发 (L) 表示</li> </ul>	➡ 数Ⅲ个人安全环境 延书	8 #11		
	主題: 主題 (各格) : ※公次:			- 1
	序列号(十六进制): 序列号(十进制):	01:00:00		
	有效期白: 算法:	01.01.2000 12:00:00 DSA	해: 01.01.2038 12:00:00 바바달로: 1024	
	图 25 算法: 校校部 (005);			<b>117</b> 94 107

点击证书下方添加到访问控制列表,系统标识输入"S4C",集团输入"700"

主题(备选):		
頭发者:		
序列号(十六进制):	01:00:00	
序列号(十进制);	65536	
有效期白:	01.01.2000 12:00:00 歪: 01.01.2038 12:00:00	
算法:	DSA 密钥强度: 1024	
签名算法:		
校验和(MD5):		
校验和 (SHA1):		
	平 添加到证书列表 击 添加到访问控制列表	
加水油能	方词控制列表 (ACL)	
	系统 类 证书主体	
Θ		
=	向単点登录访问控制列表添加条目 ×	
	*系统标识: S4C	
	*集团: <b>700</b>	
	筋有关.	
	7月11日11	
	颁发者:	
	继续 取消	
依次点击 "更多"	→ "个人安全环境" → "另存为" → "系统个人安全环境" → "继续" → "是	,,

点击右上角 "Exit" → 询问是否保存更改时点击 "是"

#### 4. 在IDaas中添加SAPGUI应用

1	添加应用								
	全部标准协	议 定制模板							
^ -									
	済加应用 本页面包含了所有已支持的可原加应用列表,管理员可以从中选择希望使用的应用进行初始化配置,并开始后续使用。								
^	■ MU用5: 定制4	▼ 加用分为期间: 一种量型持标准的 JWT、CAS、SAML 等機械的加用,在这里可以通过添加对值的标准应用模板将实现单点登录功能;另一种最定制应用,本类如用已经提供了对接其单点登录现用户同步的接口,由 DaaS 为其提供 定制化模取进行对象。							
	SAP			٩	l i i i i i i i i i i i i i i i i i i i				
~	应用图标	应用名称	标签	描述		应用类型	操作		
	-	SAP GUI	SSO, C/S	SAP GUI是SAP用户用于访问SAP系统的 软件提供商,其商品范畴包含 ERP、CRI 全球合作伙伴,广泛分布在25个不同的行	图形用户界面(Graphical User Interface)。SAP 是世界领先的企业 d、数据分析、HR、物流、差旅、金融等各方面,拥有1万8千个 业中,为各类各阶段企业提供数字化管理解决方案。	PC客户端	添加应用		
					共1条 《	( 1 > 10;	条/页 > 跳至 1		
	^	添加設用 全部 标准的 本 示理 が示加 の 本 示理 点用 の 点用 の の 、 本 の 本 の 本 の 本 の 本 の 本 の 本 の 本 の 本	<ul> <li>※初加茲用</li> <li>◆部 标准协议 定時機能</li> <li>▲部 标准协议 定時機能</li> <li>「添加应用</li> <li>本市面積高了所有已支持的可。</li> <li>加分为時年: 一般是支持板 定時代現報3時時: 一般是支持板</li> <li>SAP</li> <li>「編用間标 絵用名称</li> <li>「SAP Gui</li> </ul>	<ul> <li>         参部 标准协议 定制模板         ◆部 标准协议 定制模板</li></ul>	添加应用         金部         标准协议         並制模板           全部         标准的文         並制模板           本工商程信言 7所有已支持的可添加应用列表、管理员可以从中选择希望使用的应用进行初始化起源、并开始结构。应用分为两位: 一些是支持标准的 JWT、CAS、SAML 等模板的应用,在这里可以通过添加对应的标准应用模型的标准应用模型的标准。           SAP         Q           施用图标         雇用名称           原名         C           应用图标         雇用名称           SAP GUI         SSO, C/S           经指估件状态, 广泛为希在26个不同的方				

#### 添加应用 (SAP GUI)

应用图标	<ul> <li>         ◆ 上传文件     </li> </ul>
	图片大小不超过1MB
* 应用名称	SAP GUI
* authSchema	请填写认证Schema
	Authentication Schema
* mySysid	请填写ld
	发送方系统ID,系统的标识
* myClient	清旗写client
	反达力系统Client,头例编写
* extClient	清填写系统 client 接体主系统的Client 预持 400
	1940 ASTRUCIENT, 1944 400
* extSysid	请填写系统Id 接受方系统的ID.建议设置与 mv svsid 相同值
* host	
* 11051	应用服务器地址
SAPRouter	请填写SAPRouter
* language	请填与系统语言 SAP 系统语言 预填 E
* nortall loor	
* portaiosei	

	接收方系统门户用户 预填 PORTALUSER
* pseKeyFile	
	请上传.pse类型文件,从SAP系统中导出
* sapGuiLanguage	请填写系统语言
	sap gui 客户端语言, 预填 ZH
* sysnr	清垣与系统编号
	实例编号 预填 00
* 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

配置名称	填写值	说明
authSchema	basicauthentication	固定填写该值, SAP未给出文档解 释该值作用
mySysid	S4C	登录项中系统标识
myClient	700	登录时登录页显示的集团
ext Client	700	登录时登录页显示的集团
extSysid	S4C	登录项中系统标识
host		应用服务器地址
SAPRouter		使用到路由时填写该值,阿里给的 环境中不需要设置该值
language	E	固定填写该值, SAP未给出文档解 释该值作用
portalUser	PORTALUSER	固定填写该值, SAP未给出文档解 释该值作用
pseKeyFile	选择证书system.pse	示例给出的 system.pse 由阿里提 供;可使用 sapgenpse.exe 生 成,尽量让客户提供
sapGuiLanguage	ZH	与SAP GUI登录时登录页下方登录 语言一直
sysnr	00	实例ID

#### 5. 给应用添加子账户并审批

i. 普通用户添加子账户:

统一认证身份平台				添加子账户	
救迎 · IDaaS	应用子账户			2018.071	
主發統 ^	子账户列表 子贩户审批			104-C/1	princlemitteni 建选择关系的应用
首页 应用管理	本城 <b>庄用于账户</b> 使表在用名称		189	lest	
应用子标户	問題 放用名称	新社社会	主题户	789	789
2020 · · ·	s4-hz.chint.com	Eas	test		國家:此立用子附戶所用的星 <b>配户关联</b> 方式。如果提供正确的用户包方可整要到应用系统。
二次认证 我的简思	219823784	Bāt	best		817
我的日志	し 成本の意義	Baz	test		

ii. 管理员审批通过:

统一认证身份3	平台						消息 🕤	默认管理员→	切换语言 🗸
账户	^	审批中心							
机构及组 账户管理		子账户审批							
分类管理 认证 认证源 RADIUS	Ŷ	审批中心 审批中心是 IDaa 子账号编的是单, 审批通过后,用	S 系统中管理员集中处理所有需要 点登录时带给应用的身份标识。如 中将可以使用子账号单点登录到应	排批内容的页面,当有待审批项出现时,会在 果某应用设置纯主子账号映射关系为(于动兴 用系统中, 遗确认 IDaaS 用户主账号和子聚号	側边导航栏有数字气燃提示。 跃〕时,用户在警试单点登录的时候,如果3 的对边关系后完成审批。	2有子账号,则会提交一个子账	长号绑定申请。由管理员在	此处进行审批。	×
证书管理 授权	^	主账户 (申请人)	子账户	7月名称 待审批	◇ Q 披索 重置				
权限系统	- 1	主账户 (申请人)	子账户	应用名称	申请时间	审批状态	操作		
应用授权 分级管理		test	test	s4-hz.chint.com	2019-12-10 15:17:38	待审批	查看》	并情快速同意快速	拒绝 审批
审计	×						#1条 (	1 > 8	- 五 五
其它管理 审批中心 同步中心	^								tuda JA

6. 用户进行SAP的单点登录若提示没有安装插件,则安装插件,若有安装插件则可直接单点登录成功

统一认证身份	平台	
欢迎·IDaaS		我的应用
<b>主导航</b> 首页	^	Web应用
应用管理 应用子账户		¢ <sub>s</sub>
<b>设置</b> 我的账户 二次认证	^	s4-hz.chint.com
我的消息 我的日志		移动应用

# 1.6. OAuth2对接grafana最佳实践

#### 概述

作为IDaaS平台,IDaaS支持基于标准OAuth2协议,实现从IDaaS到graf ana单点登录 本文主要包含以下内容:

- 时序说明 时序图说明, 以及交互
- 主要流程 OAuth2配置grafana主要流程
- 操作步骤 详细配置说明
- FAQ 常见问题以及其对策

#### 时序说明

场景:用户从grafana发起单点登录时序



grafana请求时序图

# 主要流程

Step1 创建OAuth2应用 Step2 授权OAuth2应用 Step3 子账户关系配置 Step4 获取应用信息 Step5 grafana配置

#### Step6 发起登录

#### 操作步骤

Step1 创建OAuth2应用:

1、首先以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、点击左侧导航栏应用>添加应用选择右侧OAuth

统一身份认证	平台						жe တ р	线认管理员 🗸	切換語言 ~
概范 快速入门		添加应用 全部 标准协议	定利權板						
应用列表 应用列表	^	→ 添加应	行对援。		×				
用户目录 机构及组 账户管理	^	请输入应用名称				٩			
分类管理		应用图标	应用名称	应用ID	标签	描述	应用类型	1001	Bi .
认证 认证源	^	<b>\$</b>	Salesforce	plugin_salesforce	SSO	Salesforce 最在世界范围小广泛使用的公响云 CFM 平台(Customer Relationship Management,有户关系管理系统),它为企业提供了事件管理。任务管理,等件的应升级事项就的考虑重先,IDaaS 实场通过 SAML 协议单点重要到 Salesforce 网站。	Web应用	添加	加应用
RADIUS 证书管理		On *	ProcessOn	plugin_processon	SSO	ProcessOn 包用题标t (https://www.processon.com/)	Web应用	源	加应用
授权 权限系统	^	4	OIDC	plugin_oidc	SSO, OIDC	OIDC是OpenID Connect的简称。OIDC=(identity, Authentication) + OAuth 2.0, IDaaS 使用 OIDC 进行分布式站动的单点整要(SSO),	Web应用	添	加应用
应用授权	,	1	Office365-SAML	plugin_office365_saml	OA, SAML	Office365 - OA	Web应用	添加	加应用
其它管理	v	OLL TH	OAuth2	plugin_oauth2	OAuth2	OAum 是一个开始的资源接份协议,应用可以通过 OAum 获取到全藏 access_token,并拥有全棘中服务装造农用户资源,应用可以使用 OAum 应 用模拟中实现统一条合管理。	Web应用	(数)	加成期
设置	×	J	jwti迂书	plugin_jwtcert	SSO, JWT, SCIM	jut至2029d_boken包含还书信息	Web应用, 移动应用, PC	<u>客户纳</u> 液)	加应用
		sts	JWT STS(附网关保护)	plugin_jwt_sts	STS, JWT	JWT STS, 支持局关码户, 至我JWTF与检验JWT	Web应用	源	加应用
		J	JWT_ALG	plugin_jwt_alg	SSO, JWT, HS256	JWT (JONI Wab Taken) 最石洞扇应用石積和間約-兩級子-ISON 約开設活動。Das5 使用 JWT 更行分布式达动的最单量类(SSO)、JWT 集合整要最子对称如果。由 Das5 将用小状态和透整使用弯相如果,像激响应用后,应用使用弯钢等常并进行验证。使用马属6家/T-E、集成器 集。	Web应用, 移动应用, PC	<u>你户纳 汤</u> 3	加应用
						JWT(JSON Web Token)是在网络应用环境声明的一种基于 JSON 的开放标准。IDaaS 使用 JWT 进行分布式站点的单点整要(SSO),JWT			

#### 3、选择OAuth2应用模板点击添加应用。

统一身份认证平台			修改应用 (OAu	ith2)			
选 wm ) C	应用列表		NAME WYNLLYJAN 出用户安全级别低于应用需求时,调用此处指定的方式进行到化认证。				
(墨入口) 7用 ^ 应用列表	应用列表 管理员可以在当前页面管理已经添加的所有 当添加完应用后,应该确认应用处于应用状	应用,应用可以实现 <b>单点登录和数据同步</b> 能力。 态,并已经完成了授权。在应用详情中,可以看到	*应用类型	✓ Web应用 ✓ 終功应用 ✓ PC客户端 Web应用"IT"C名户端只会在用户Web使用环境中显示,"移动应用"只会在用户案户算中显示,如用 个环境中都显示应用局动选多个。			
添加应用 1户目录 へ	<b>送加於用</b> 補給入成用名称		* Redirect URI	http:/=Kvv=*114K3oilogin/generic_oauth			
机构及组账户管理	应用图示 应用名称	DI肝设	SP HomePageURL	OAuth2 Redirect URI, 請以 https: 开头。 词始ASP HomePageURI。			
分类管理	OAuth2	idaasplugin_oauth2		应用首页地址,支持手动拨起SSO。			
认证源 RADIUS	应用信息	账户信息 - 同步	* GrantType	authorization_code Authorization_code: 医权利姆式 (即先登录获取Code,再获取Token) , 领电OAuth2流程; Implicit: 这 (在Rediced: unixhtashfräToken) 适用于验证第二方合法社创使用; PKCE 量于使好研模式的一 展 主要适用于无后端感务需未能改化处理Authorization Code提权研的应用, 应用决定加密方式并当			
业书管理 訳 ^ 权限系统	应用的详细信息 查看详情 特改应用 删除应用	SCIM的议设置以及把组织机构、组同步 用 同步机构 SCIM配置	Access_Token有效期	文、IDP通过花絵館文好合成社業利期後20月8月4日。 <b>7200</b> Access_Token的有効設計に(単位: 秒)、飲以357200(2小社)			
应用授权	审计信息	API	Refresh Token有效期	804800 Refresh Token的有效因时长(师位: 秒), 默认为5604800(7天)			
它管理 <sup>●</sup> ~	查看应用系统详细的操作日志 查看同步记录	是否对应用开放系统API	授权码CODE有效期	60 授权码CODE的有效图长(单位: 秒),就认为60(1分钟)			
				103H			

4、Redirect URI:http://{graf ana domin}/login/generic\_oauth {} 替换成graf ana的域名地址

GrantType:选择authorization\_code

其他参数默认即可,有需要也可按照实际需要修改

#### Step2 OAuth2应用授权

应用授权:选择应用(搜索应用)、选择组织机构(搜索组织机构)、勾选授权即可

#### 单点登录配置·最佳实践

既览		应用授权
央速入门		按应用摄权组织机构/组 按组织机构/组授权应用 按账户援权应用 按应用援权账户 按分类授权应用
立用 应用列表 添加应用 形户	^	应用授权 ☞ 管理员可以在这里使用不同方式为应用进行授权分配。 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;也可以选定一个账户,并为其分配有权限访问的应用列表。
机构及组 账户管理 分类管理		应用 (1) 组织机构和组 (1) 已版权(1)个 请输入应用名称进行查找 Q
从证 认证源 RADIUS 证书管理	^	OAuth2 → 請输入名称进行搬索 共1条 〈 1 >
愛取 权限系统 应用授权	^	
新计	~	
<b>其它管理</b>	~	
受置	~	

#### Step3 子账户设置

点击左侧导航栏应用>应用列表>应用子账户 查看 OAuth2,添加子账户对应关系。

主账户添加当前已经授权应用的IDaaS账户,子账户对应grafana的邮箱用户,需要一一对应。

#### ? 说明

子账户一定需要填写邮箱用户。

概览		应用列表 / <b>子账户</b>								
快速入门		←子账户 和限分类 離星 化化合成 化合成 化合成 化合成 化合成 化合成 化合成 化合成 化合成 化合								
应用	^									
应用列表 添加应用 用户目录 机构及组	^	子発产 子祭产指的是在指地应用系统中,用户会以什么身份进行访问。主祭产指的是 DaaS 中的账户。在进行集成登录时,DaaS 会向应用系统传递对应的子祭户,该子祭产需要在应用系统中并在且可识别。 举例:DaaS 中专主祭产 発圧 (用户名 zhangsan),在企业的 BPM 应用系统中,这个用户的用户名是 agoodman,即子祭产馆为agoodman,与主祭产 zhangsan 进行关联。 聚户关联方式:在应用创建时,如果选择了祭户领封,即款以主祭户和子祭户完全一致,无需能置。如果选择了祭户关联,购需要在这里进行手动的子祭户创建和主子祭户关联。								
账户管理 分类管理		OAuth2								
认证 认证源	^	主影户 (勝户名称) Q								



#### Step4 获取应用信息

点击左侧导航栏应用>应用列表 查看 OAuth2 应用详情,获得Client Id、Client Secret、Authorize URL.

		应用列表							应用分类
概范		100007944							
<b>应用</b> <b>运用列表</b> 添加应用	Ŷ	应用羽 管理別 当添加	列表 员可以在当前页面管理已经添加的所有应用,应用可以实现单点 印完应用后,应该确认应用处于但用状态,并已经完成了接权。	登录仰题编码步能力。 在应用评情中,可以看到应用的评细信息、单点登录地址、子	账户配置、同步看	遭、授权、审计等信息 <b>。</b>			×
用户目录	^	添加应用	青榆入应用名称		٩				
机构及组 账户管理		应用图标	应用名称	应用iD	应用分类		应用状态	二次认证状态	操作
分类管理		J	JWT1126	no and th					授权 洋情 ▼
认证课	Ŷ	J	JWT1120						授权 详情 ▼
证书管理		ONTH	OAuth2题试	2032/25-221	统计分类				授权 详情 •
授权	^								
权限系统		应用信息		账户信息 - 同步		账户信息 - 子账户		授权信息	
auroletx 审计		应用的详细	的思	SCIM协议设置以及把组织机构、组同步推送至应用		平台主账户与应用系统中子账户的关联课		应用与人员组织的授权关系	
其它管理	~	童君洋情	你改立用 删除应用	同步机构 SCIM配置		查看应用子账户		授权	
设置	~								
		审计信息		API		管理应用内权限			
		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			

应用详情 (OAu	th2测试)
图标	OAUTH
应用ID	1000-05400-0
应用名称	OAuth2测试
应用Uuid	
安全等级	5
	请设置应用的安全等级,数字越大表示需要的安全等级越高,与认证源安全级别挂钩。
指定认证方式	<b>原随系统</b> ~
	当用户安全级别低于应用需求时,请用此处描定的方式进行强化从证。
应用安全等级	无
Client Id	
Client Secret	
Redirect URI	
SP HomePageURL	
GrantType	authorization_code
Authorize URL	https:// 📲 💼 👘 manager.com/oauth/authorize?
	response_type=code&scope=read&client_id=%11fff111 peri h111ff17 % 6%2001 host 7%41201 operative Sea (_ periodea from the Chemical Periodea
	om&state====1000,000 mm/mm/mm/mm/mm/mm/mm/mm/mm/mm/mm/mm/mm/

#### Step5 grafana配置

1.grafana配置文件增加generic\_oauth配置

vim /etc/grafana/grafana.ini

#generic\_oauth配置

[auth.generic\_oauth]

enabled = true

#IDaaS应用Client Id

client\_id =57064exxxxxxxxxx

#IDaaS应用Client Secret

client\_secret =PTsclAxxxxxxxxxx

scopes = read

#IDaaS授权url,需要替换为自己的实际的IDaaS的域名

auth\_url =http://xxxxx.login.aliyunidaas.com/oauth/authorize #IDaaS获取token url, 需要替换为自己的实际的IDaaS的域名 token\_url =http://xxxxxx.login.aliyunidaas.com/oauth/token #IDaaS获取 user info url, 需要替换为自己的实际的IDaaS的域名 api\_url =http://xxxxxx.login.aliyunidaas.com/api/bff/v1.2/oauth2/userinfo allow\_sign\_up = true #获取邮箱节点JMEpath email\_attribute\_path=data.email [server] #这里的root\_url需要修改为真实的地址,因为授权回调的redirect\_uri使用该地址 root\_url=http://xxxxxx:3000 2. 重启grafana 示例: /etc/init.d/grafana-server restart 根据自己实际安装路径来 **Step6 grafana发起OAuth登录** 

#### ? 说明

grafana使用OAuth2对接,只支持grafana页面发起登录,不支持 IDaaS发起

#### 在grafana登录页面点击 "Sing in with OAuth" 发起认证登录

<b>C</b>	
Welcome to Grafana Your single pane of glass	
Email or username email or username Password password	lt
Log in Forgot your password?	
or Sign in with OAuth	
Documentation        O Support        Community   Open Source   v7.3.4 (14c494085e)	•

输入IDaas账号进行登录

简体中文	扫码登录更便捷	
		X
法法 》 影片 /	阿里云IDAAS	
请输入来四		
	忘记室码	
	提交	
×	V V	
	7	

### 认证成功



# FAQ

1. 代理模式下报错如下

OAuth认证错误: error="invalid\_grant", error\_description="Invalid

redirect:http://localhost:3000/login/generic\_oauthdoes not match one of the registered values: [http(https)://域名/login/generic\_oauth]"。

代理模式(nginx或者apache),需要在grafana.ini中修改 redirect URI。因为代理模式下,不认识CALLBACK

Redirect URI:http://{grafana domin}/login/generic\_oauth {} 替换成grafana的域名地址

2. 子账户对应关系是否需要一对一

是的。

3. Grafana 支持的版本

需要grafana7.2+版本才能兼容此OAuth2的配置。

# 1.7. Jenkins对接(SAML)

通过 IDaaS 提供的单点登录能力,快速实现Jenkins 单点登录的目的。

#### 操作步骤

1、在 Jenkins 插件管理中安装 saml 插件。

2、在 Jenkins 中进入"Configure Global Security",在"Authentication"中选择"SAML 2.0"。

3、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。

4、在云盾IDaaS管理平台中左侧菜单中点击添加应用,找到"SAML"应用,点击"添加应用"。

加	^	•	C/S程序(浏览器)	plugin_cs_multibrowser	CS, PC, Multi Browser	唤醒指定浏览器打开指定系统,并通过模拟操作行为的方式进行代填登录,适用于只能用指定浏览器(IE/谷歌)火狐/搜狗/360等)打开的应用	PC客户端	添加应用
应用列表 添加应用			CAS(标准)	plugin_cas_apereo	SSO, CAS	CAS (Central Authentication Service,集中式认证服务,版本2.0)是 一种基于挑战、应答的开源单点登录协议。在集成客户端和服务端之间 网络通畅的情况下广泛在企业中使用,有集成简便,扩展性强的优点。	Web应用, 移动应用	添加应用
11户目录 机构及组 账户管理	^	J	JWT	plugin_jwt	SSO, JWT	JWT (JSON Web Token) 是在网络应用环境冲明的一种基于 JSON 的 开放标理。[Dass 使用 JWT 进行分布式达点的单点容量(SSO)。 JWT 单点容量基于建对称加密。由 IDass 将用户状态和信息使用私销加 密、传递给应用后,应用使用公明解密并进行验证。使用场景非常广 泛,集成简单。	Web应用, 移动应用, PC客户端	添加应用
分类管理 人证	~	OAUTH	OAuth2	plugin_oauth2	OAuth2	OAuth 是一个开放的资源授权协议,应用可以通过 OAuth 获取到令牌 access_token,并携带令牌来服务端请求用户资源。应用可以使用 OAuth 应用模板来实现统一身份管理。	Web应用	添加应用
认证源 RADIUS		C.	OIDC	plugin_oidc	SSO, OIDC	OIDC是OpenID Connect的简称,OIDC=(Identity, Authentication) + OAuth 2.0。IDaaS 使用 OIDC 进行分布式站点的单点登录 (SSO)。	Web应用	添加应用
证书管理 受权 权限系统	^	SAME	SAML	plugin_saml	SSO, SAML	SAML (Security Assertion Markup Language, 安全新苦香店记语声, 既 本 20) 基于XAM 协议。使用检查新语(Assertion) 的安全会确, 在睡 权方 (IDaaS) 和周藤方 (应用) 之间传递单份信息。实现基于间端跨 地方确认错录。SAML 协议是成绩培认证协议, 在国内外给公有云和私 有云中有主带了达的运用。	Web应用	添加应用
应用授权 a计 吃管理	~	*	SAP GUI	plugin_sap_gui	SSO, C/S	SAP GU是SAP用户用于访问SAP系统的图形用户界面(Graphical User Interface), SAP 是世界领先的企业软件提供商,挑构品证确有含 ERP、CRM、数量分析、HR、物质、差版、金融等各方面,拥有1万8 千个全球合作伙伴,广泛分布在266个不同的行业中,为结类者阶段企业 提供数字化管理解决方案。	PC客户端	添加应用

5、在证书界面点击"添加SigningKey"。在名称中输入一个便于标识的证书名称,如"Jenkins";国家选择"CN";省份任意填写,如"Beijing";证书长度选择"2048";有效期选择"3年"。

添加应用 (SAML)	添加SigningKey		>
民) SigningKey			
	* 名称	Jenkins	
别名	部门名称	请输入部门名称	
CN=test, ST=test, C=C	公司名称	请输入公司名称	
	* 国家	CN	~
	* 省份	Beijing	
	城市	请输入城市	
	* 证书长度	2048	~
	* 有效期	3年	~
		<b>提交</b> 取消	

6、添加完成后会自动回到证书列表界面, 在刚才添加的证书右边, 点击"选择"。

2	励应用(SAML)						$\times$
	导入SigningKey 凝	តិវ៉ាពSigningKey					
	别名	序列号	有效期	秘钥算法	算法长度	操作	
	CN=test, ST=test, C=CN	3411728164704371020	1095	RSA	2048	选择 导出	
	CN=Jenkins, ST=Beijing, C=CN	5980551192585266966	1095	RSA	2048	选择导出	

- 7、添加应用页面参数
- 应用名称填写便于识别的名称,如 "Jenkins";
- IDaaS IdentityId 填写任意文字,如"IDaaS";
- SP Entity ID 填写任意文字,如 "Jenkins"; SP ACS URL(SSO Location) 填写任意地址; NameldFormat 选择第一个,即 "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified";
- 若Jenkins中员工用户名与IDaaS系统中员工用户名一致,则选择账户映射,否则选择账户关联; 点击"提交"添加成功。

* 应用名称	Jenkins
* IDaaS IdentityId	IDaaS
	IDaaS IdentityId is required
* SP Entity ID	Jenkins
	SP Entity ID is required
* SP ACS URL(SSO Location)	https://admin.idp& Mineranger.nom
SP 登出地址	请输入SP 登出地址
* NameldFormat	um:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Assertion Attribute	Assertion Attribute key - +
	断言属性。设值后,会将值放入SAML断言中。名称为自定义名称,值为账户的属性值。
Sign Assertion	
IDaaS发起登录地址	IDaaS发起登录地址
	以 http://、https:// 开头, 填写后使用 IDaaS 发起登录将会跳转到该地址, 而不会使用 SAML 的idp发起登录流 程
* 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)

8、添加完成后将会提示对应用进行授权。点击"立即授权",进入应用授权界面,可根据需求按组织机构、账户等对应用进行授权,授权后的组织机构/账户才能够登录该应用。勾选需要授权的组织机构/账户

后,在页面最下方点击保存,并在弹出的确认窗口确认授权。

# 系统提示

应用添加成功,尚未分配权限,如需对应用进行授权 请点击"立即授权"。



9、在IDaaS中进入应用列表页面,可看到刚才添加的应用。点击右侧详情,点击查看详情,可查看需要在 Jenkins中配置的信息,点击"导出 IDaaS SAML 元配置文件"下载 IDaaS 元配置文件,使用记事本打开该文件,复制所有内容待用。

10、使用具有管理员权限的用户登录到 Jenkins 系统中,依次点击"Manage Jenkins"、"Configure Global Security",进入"Configure Global Security"。在"Security Realm"中,选择"SAML 2.0",在"IdP Met adat a"中粘贴第 9 步复制的 IDaaS 元配置文件内容,点击"Save"。

应用身份服务

单点登录配置·最佳实践

Security Realm		
$\bigcirc$ CAS (Central Authentication	Service)	
<ul> <li>Delegate to servlet containe</li> </ul>	r	
○ Jenkins' own user database		
SAML 2.0		
IdP Metadata	<md:entitydescriptor er<br="" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"><md:idpssodescriptor <br="" wantauthnrequestssigned="false">protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"&gt; <md:keydescriptor use="signing"> <ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:x509data> <ds:x509data> <ds:x509certificate>MIIC4jCCAcqgAwlBAgIIUv8vn5MVZxYwDQYJKoZlhvcN UEBhMCQ04xEDAOBgNVBAgTB0JlaWppbmcxEDAOBgNVBAMTB0plbmtpb OTU2WhcNMjMwNjE3MTAxOTU2WjAxMQswCQYDVQQGEwJDTjEQMA4GA MA4GA1UEAxMHESmVua2luczCCASIwDQYJKoZlhvcNAQEBBQADggEPADCC NmsDx7S3FqSFl2wQ/XQTqIXIpNQzaY0Znh+JKDr2dn7V3gyj1lnNXX/q4yuj/t kQLKI6P7ht7AyD82JY4Rcz2HWzrzgKXQHP8EshS5LobLwsylzsTYrSjIKijd5pDL bnjINvlyqxD8+ZKr1QyQDGUxKUAh/cVb+orf4zwgcj1koAtAt17Zpsaj+SLbbC afBmyMbIf6sNPuA5Ya33yqYKremZNFbMSQEZVPMZh36bbv57JdIIST8L0Sv0 CAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAKX6SCEUsySX00IqMJPP3qaM Q9p3XK8+rKGCtKsx4ZCoaVpUs6P2mdIcv34R2C0mHdefAlUn2gilkphtYLpM NwNQnyBUtDH1TQA1BRqTV6Yd47HRhCPUXCr8+1r57NxwlsrUbJYRWHAGI e0UHUHDMZDe19OYDPQ8qkjE0duft1q4253sLoUrZF2xe8b35fv3fcmPbMu+ u0CCN489IzGdt1TNeYg3EvvXbl4JSTyoq1woJ2pbIKC2HsiohOHvBSWFe8ewv </ds:x509certificate></ds:x509data></ds:x509data></ds:keyinfo></md:keydescriptor></md:idpssodescriptor></md:entitydescriptor>	ntityID="IDaaS"> JAQEFBQAwMTELMAkGA1 nMwHhcNMjAwNjE3MTAx 1UECBMHQmVpamIuZzEQ AQoCggEBAIDuOw8KJa1o nrY96Dxraon4InOAVNIIy0K egAZsDyI0me61AE6xf51nP DtmaukAGMqwShkD4Mwle +4m3M1jh9NdMKrY0/LIM luTQIUJ/nhuo6NwxVk/RJo ZG6sZXsZhyB8suARL5fh+ B+VoD/yEGDxd4Wb6TUBEi eUjO+Ei8kb+9oRQk5AWgX w==
	Raw Xml IdP Metadata	
		Validate IdP Metadata

11、重新进入"Configure Global Security"。点击"SAML 2.0"下方"Service Provider Metadata",打开 Jenkins SAML元配置文件。

	Minutes between downloads of the IdP Metadata	
	Validate IdP Metadata U	JRL
Display Name Attribute	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	_
Group Attribute	http://schemas.xmlsoap.org/claims/Group	
Maximum Authentication Lifetim	e 86400	
Username Attribute		
	▲ It is recommended to set the username attribute.	
Email Attribute		
	▲ It is recommended to set the email attribute.	
Username Case Conversion	None 🗸	
Data Binding Method	HTTP-Redirect V	
Logout URL		
	Advanced Configuration	
	Encryption Configuration	
Custom Attributes	Add -	
Service Provider Metadata v hich	may be required to configure your Identity Provider (based on last saved settings).	
⊖ None		

12、在"Service Provider Metadata"数据中找到"entityID",将后面引号中的值, 如"http://11.167.179.25:808/securityRealm/finishLogin",复制待用;在"Service Provider Metadata"数据中找到"AssertionConsumerService",将后面"Location="后引号中的值, 如"http://11.167.179.25:8080/securityRealm/finishLogin",复制待用。

13、在 IDaaS 中进入应用列表页面,找到添加的应用。点击应用状态下方按钮,禁用应用,在弹出的确认框中点击"确定"。

Ŵ	应用列表 管理员可以在当前页面管理已经添加的所有质 当添加完成用后,应该确认应用处于启用状。	立用,应用可以实现 <b>单点登录和数据同步</b> 能 5,并已经完成了授权。在应用详情中,可	幼。 [以看到应用的详细信息、单点登录集	助此、子账户配置、同步配置、授权、	审计等信息。	
请输入应用	相名称		Q			
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
SAME	Jenkins	adminplugin_saml2	Web应用		×	授权 详情 ▼
☞	应用列表 管理员可以在当前页面管理已经添加的所有后 当添加完应用后,应该确认应用处于启用状绪 经条	? 系统提示 确认禁用应用(J 5.并已。	enkins) ? <b>确定</b> 1	"配置、同步配置、 授权、 取消	审计等信息。	
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
SAML	Jenkins	adminplugin_saml2				授权 详情 🔻

14、点击应用右侧详情按钮,点击"修改应用"。

请输入应用名称			Q				
应用图标	应用名称	应用ID	设备类型	应用状态	_2	灾认证状态	操作
SAML	Jenkins	adminplugin_saml2	Web应用	×	C	×	授权 详情 🔺
应用信息		认证信息		账户信息 - 同步		账户信息 - 子账户	
应用的详细信	志	应用的单点登录地址		SCIM协议设置以及把组织机构、组同步推进	送至应	平台主账户与应用系统中	子账户的关联表
查看详情	修改应用 删除应用	IDaaS发起地址		用步机构 SCIM配置		查看应用子账户	
授权信息		审计信息		API		管理应用内权限	
应用与人员维	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校	限
授权		查看日志 查看同步记录		API Key API Secret		绑定权限系统	

15、在"SP Entity ID"中填写第 12 步复制的"entityID"的值;在"SP ACS URL(SSO Location)"中填写第 12 步复制的"Location="的值,点击提交。

应用ID	adminplugin_saml2
* 应用名称	Jenkins
* IDaaS IdentityId	IDaaS
* SP Entity ID	http://11.167.179.25:8080/securityRealm/finishLogin
2	SP Entity ID is required
* SP ACS URL(SSO Location)	http://11.167.179.25:8080/securityRealm/finishLogin
SP 登出地址	请输入SP 登出地址
* NameldFormat	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Assertion Attribute	Assertion Attribute key
	断言属性。设值后,会将值放入SAML断言中。名称为自定义名称,值为账户的属性值。
Sign Assertion	
IDaaS发起登录地址	IDaaS发起登录地址
	以 http://、https:// 开头, 填写后使用 IDaaS 发起登录将会跳转到该地址, 而不会使用 SAML 能程
* 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)

#### 修改应用 (Jenkins)

16、回到应用列表界面,点击应用状态下方按钮,启用应用。

17、使用新的浏览器打开 Jenkins 地址 将会跳转到 IDaaS 进行登录,在 IDaaS 登录成功后,会跳转回 Jenkins。

# 1.8. WordPress对接

### 一、WordPress-SAML应用

WordPress-SAML应用主要实现支撑单点登录流程的功能。

操作步骤:

 $\times$ 

- 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. 点击左侧导航 应用 > 添加应用,选择WordPress-SAML应用模板点击添加应用.。
- 3. 点击 添加SigningKey。

添加应用 (WordPress-SAML)

导入SigningKey 添加SigningKey					
Alias	SerialNumber	ValidityDays	KeyAlgorithm	KeySize	操作
CN=ceshi, OU=asd, O=asdsad, L=asd, ST= asd, C=CN	2972402420277091813	180	RSA	1024	选择 导出
CN=wordPress610, ST=四川, C=CN	8919955222722806429	365	RSA	2048	选择导出
CN=ceshi624, ST=四川, C=CN	1666666283299562331	365	RSA	2048	选择 导出
CN=d, ST=SC, C=CN	8429590403889353502	180	RSA	2048	选择 导出

4. 点击选择进入添加应用页面

	命 上传文件
	图片大小不超过1MB
应用ID	wceshiwordpress_saml2
SigningKey	e02519860ccb392832b90f2facd36dd9zk5Wko5xAYa
* 应用名称	WordPress-SAML
* 所属领域	请选择
* 应用类型	Web应用
* IDaaS IdentityId	请输入IDaaS IdentityId
	IDaaS Identityld is required
* SP Entity ID	请输入SP Entity ID
	SP Entity ID is required
* SP ACS URL(SSO Loc ation)	请输入SP ACS URL(SSO Location)
SP 登出地址	请输入SP 登出地址
⊧ NameldFormat	<sub>请选择</sub> 激活 Windows <sup>×</sup>
* Binding	表到 以且 以就心 WINDOWS。 POST ✓
⑦ 说明 其中IDaaS Id	entity ld任意填写,填写后的任意值同步到WordPress里,SP Entity ID、SP

二、WordPress-SAML配置流程

WordPress-SAML在php环境中运行的,因此需要搭建一套php的环境,操作步骤如下:

ACS URL、Name ld Format所对应填写参数的值要在WordPress里面获取;

- 1. 官网下载WampServer并进行解压;
- 2. 官网下载WordPress解压后放置WampServe的www目录下

📕   🗹 📕 =	www							-	
文件 主页	共享	查看							^
★ 复制 (快速访问)	<mark>亡</mark> 粘贴	★ 剪切 ● 复制路径 ■ 和助けまです。	移动到 复制到 <b>删除</b> 重命名	▲ 新建项目・ ① 轻松访问・ 新建 文件夹	▲ 打开 · 届性 ▲ 打开 · ◎ 编辑 ◎ 历史记录	<ul> <li>         → 全部选择         <ul> <li></li></ul></li></ul>			
	剪贴板		组织	新建	打开	选择			
$\leftarrow  \rightarrow  \checkmark  \uparrow$	<mark>│</mark> > ;	这台电脑 > Winc	dows (C:) > wamp > www					~ Ū	搜索"www",
📙 桌面	* '	名称	^	修改日期	Я	类型	大小		
📜 下载	*	📕 wampla	inques	2019/6	/10 17:06	文件夹			
📔 文档	*	wampth	nemes	2019/6	/10 17:06	文件夹			
📙 图片	*	📕 wordpr	ess	2019/6	/10 17:22	文件夹			
🙆 OneDrive		add_vho	ost.php	2016/8	/16 18:02	PHP 文件	18 KB		
		😡 favicon.	ico	2010/1	2/31 9:40	图标	198 KB		
🍤 这台电脑		index.p	hp	2016/8	/16 18:03	PHP 文件	30 KB		
📙 3D 对象		test_so	ckets.php	2015/9	/21 17:30	PHP 文件	1 KB		
📱 视频		📄 testmys	sql.php	2016/5	/17 15:58	PHP 文件	1 KB		
📙 图片		🔛 wordpr	ess-5.2.1.zip	2019/6	/10 17:14	WinRAR ZIP 压缩文件	11,836 KB		
📔 文档									
📘 下载									
🜗 音乐									
■ 桌面									
Survey Windows	s (C:)								

3. 在mysql中创建一个WordPress账户;

#### 4. 在WordPress欢迎页面,设置用户名和密码

### 欢迎

欢迎使用著名的WordPress五分钟安装程序! 请简单地填写下面的表格,来开始使用这个世界上最具扩展性、最强大的个人信息发布平台。

需要信息	
您需要填写一些基本信息	。无需担心填错,这些信息以后可以再次修改。
站点标题	
用户名	
	用户名只能含有字母、数字、空格、下划线、连字符、句号和"@"符号。
密码	1000 隠蔵
	强
	重要: 您将需要此密码来登录, 请将其保存在安全的位置。
您的电子邮件	
	请仔细检查电子邮件地址后再继续。
对搜索引擎的可见性	建议搜索引擎不索引本站点 搜索引擎将本着自觉自愿的原则对待WordPress提出的请求。并不是所有搜索引擎都会遵守这类请求。
安装WordPress	

- 5. 点击左下角 "安装WordPress" 按钮;
- 6. 下载miniorange-saml-20-single-sign-on.4.8.23,将其解压后放置C:\wamp\www\WordPress\wp-

content\plugins路径下面

📕   🗹 📕 =	plugins						-		×
文件 主页	共享	查看							^ ?
★ 固定到" 复制 快速访问"	おいたのでは、	。剪切 复制路径 】粘贴快捷方式	移动到 复制到 <b>删除</b> 重命	▲ 名 新建 文件夹 ▲ 小 二 日 新建项目 ・ 1 全 松访问 ・ 、 本 建 、 の ・ 、 、 、 、 、 、 、 、 、 、 、 、 、	<ul> <li>↓</li> <li>↓</li></ul>	➡ 全部选择 册 全部取消 ■ 反向选择			
	剪贴板		组织	新建	打开	选择			
$\leftarrow  \rightarrow  \checkmark  \uparrow$	<mark>▶</mark> > 这	这台电脑 > Wind	lows (C:) > wamp > www	v > wordpress > wp-con	tent → plugins		~ Ŭ	搜索"plu	<i>م</i>
📙 桌面	* ^	名称	^	修改日期	类型	大小			
🖡 下载	*	akismet		2019/5/22 2:25	文件夹				
📔 文档	*	📜 miniora	nge-saml-20-single-sign-o	n 2019/6/10 17:25	文件夹				
🔚 图片	*	hello.ph	ip	2019/3/19 1:19	PHP 文件	3 KB			
\land OneDrive		index.pl	hp	2014/6/5 23:59	PHP 文件	1 KB			
🔎 这台电脑									
📙 3D 对象									
■ 视频									
📙 图片									
📔 文档									
🚺 下载									
🜗 音乐									

7. 重启php环境 "restart all services",然后安装miniorange并启用,首先登录WordPress进入页面点击"插件"进入页面,点击miniorange下面的"启用"按钮,然后刷新一下页面。

Ⅲ 应用   在线JSON	校验格式化 🗋 EndUser	Portal API SON在	浅解析及推測 🗛 企业微信 🧧 九州云鶴		
🔞 🔂 test 🛡 0	+ 新建				🛤, admin 🔲
4월 仪表盘	插件 安装播作	ŧ		显示选项 ▼	帮助 🔻
★ 文章	全部(3)   启用	(1)   未启用 (2)	搜索已安装	的插件	
9)媒体	批量操作 • 应	用			3个项目
■ 東面 ■ NEXA	□ 插件		图像描述		
♥ ¥12 ▶ 外观	Akismet Akism	nti-Spam	由千百万人使用,Akismet可能是保护您的站后免受垃圾评论 <b>的世界上最好的方式</b> ,它会不断地保护您的站点。使用方式:激活Akismet循件,然后碎到 密钥。 4.12版本  由Automatic   查看评情	kismet设置页面来:	Q置您的API
已安装的插件 安装插件	miniOrang 停用	e SSO using SAML 2.0	miniOrange SAML 2.0 SSO enables user to perform Single Sign On with any SAML 2.0 enabled identity Provider. 4.823版本   由miniOrange   访问顺件主页		
Plugin Editor	□ 你好多莉		这不是普通的插件,它象征着一代人希望和热情,浓缩或Louis Armstrong的四个字:你好,多和,在启用后,在您站点后台每个页面的石上角都可以看到	一句来自《俏红娘	會乐剧的
🎍 用户	<b>启用</b> 删除		與人朋戚旨词。 1.7.2版本   由Matt Mullenweg   责看评情		
<b>₽</b> IQ	115//1		20.净结;4		
en iem			INTERNITY.		
iminiOrange SAML 2.0 SSO	批量操作 • 应	用			3个项目

8. 页面会弹出miniorange saml选项

$\leftarrow$ $\rightarrow$ C $\triangle$ O local	nost/wordpress/wp-admin/admin.php?page=mo	saml_settings&tab=config	
👖 应用 🌗 在线JSON校验机	武化 🗋 EndUser Portal API() 🔤 JSON在线解析及档式	💫 企业微信 📒 九州云腾	
🔞 🖀 test 🗭 0 🕂 🕏	后建		RB,
429 仪表盘	Warning: <u>PHP openssl extension</u> is not installed or disable	d)	
★ 文章	Account Setup Identity Provider Service P	rovider Attribute/Role Mapping Help & FAQ Licensing Plans	
9] 媒体			Support
📕 页面	Please Register or Login with miniOrange to configure	the miniOrange SAML Plugin.	Need any hele 2 We are hele you with an few ine your Identity (
₽ 评论	Step 1:		Just send us a query and we will get back to you soon.
▶ 外观	You will need the following information to configure	your IdP. Copy it and keep it handy:	Enter your email
▶ 插件			<b>■ *</b> +1
• 用户	SP-EntityID / Issuer	http://localhost/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/	Write your query here
▶ 工具	ACS (AssertionConsumerService) URL	http://localhost/wordpress/	
い 没有	Audience URI	http://localhost/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/	提交
2.0 SSO ● 收起菜单	NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress	
	Recipient URL	http://localhost/wordpress/	
	Destination URL	http://localhost/wordpress/	
	Default Relay State (Optional)	http://localhost/wordpress/	
	Certificate (Optional)	Download (Register to download the certificate)	激活 Windows 转到"设置"以激活 Windows

9. 将Identity Provider页面中SP-EntityID/Issuer、ACS(Assertion Consumer Service)URL、Name ID format的值填写到IDP4"添加WordPress-SAML"页面

	命 上传文件			
	图片大小不超过1MB			
应用ID	wceshiwordpress_saml2			
SigningKey	e02519860ccb392832b90f2facd	36dd9zk5Wko5xAYa		
* 应用名称	WordPress-SAML			
* 所属领域	请选择		~	
* 应用类型	Web应用			
* IDaaS IdentityId	请输入IDaaS IdentityId			
	IDaaS IdentityId is required			
* SP Entity ID	请输入SP Entity ID			
	SP Entity ID is required			_
* SP ACS URL(SSO Loc ation)	请输入SP ACS URL(SSO Loca	tion)		
SP 登出地址	请输入SP 登出地址			
∘ NameldFormat	请选择	激活 Windows	~	
* Binding	POST	转到 反自 以激洒 WINDOWS。	~	

10. 其中IDaaS Identity Id的值任意填写,填写后的值同步到WordPress的Service Provider页面进行对应,最后将IDP4中的cer文件导入到WordPress中的X.509 Certificate中

identity Provider	Service Provider	Sign in Settings	Attribute/Role Mapping	Help & FAQ	Licensing Plans	
Configure Servi	ce Provider					
Enter the information	n gathered from your le	dentity Provider				
Identity Provider Na	me *: 123					
IdP Entity ID or Issue	er *: http://	/idass-local.com/idass				
SAML Login URL *:	http://	íidass-local.com/idass				
X.509 Certificate *: MIIC6jCCAdKgAwlBAglle8oMA97lgp0wDQYJKoZlhvcNAQEFBQAwNTELMAkGA1UE BIMCQQ4xDzANBgNVBAgMBuWbm+W3nTEVMBMGA1UEAxMMd29yZFByZXNzNjEwMB4X DTE5MDYxMDA4MDEyNFoXDTIwMDYwOTA4MDEyNFowNTELMAkGa1UEBhMCQ04xDzAN					Î	
	DIESI				DIIWCQU4XDZAW	11
	NOTE: F	ormat of the certificate GIN CERTIFICATE XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	XXXXX			11
Response Signed:	NOTE: F BE XXXXXX EN	ormat of the certificate SIN CERTIFICATE XXXXXXXXXXXXXXXXX D CERTIFICATE ck if your IdP is signing	: XXXXX the SAML Response. Leave che	cked by default.		<i>li</i>
Response Signed: Assertion Signed:	NOTE: BE XXXXXX EN ✓ Che	ormat of the certificate SIN CERTIFICATE 000000000000000000 D CERTIFICATE ck if your IdP is signing tck if the IdP is signing 1	: XXXXX the SAML Response. Leave che he SAML Assertion. Leave unch	cked by default. ecked by default.		X
Response Signed: Assertion Signed:	VOTE: 1 NOTE: 1 X00000 ·····EN ♥ Che Che	ormat of the certificate SIN CERTIFICATE OXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	: XXXXXX the SAML Response. Leave che he SAML Assertion. Leave unch guration	cked by default. ecked by default.		X

11. 配置完成之后,选择WordPress-SAML应用添加应用子账户,子账户是wordpress中账号的邮箱,即可单 点登录WordPress。

#### 补充

1. 本地部署的wordpress的url地址为127.0.0.1或localhost,可以在设置中修改wordpress的url地址。

You will need the following information to configure your IdP. Copy it and keep it handy:

SP-EntityID / Issuer	http://127.0.0.1/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/
ACS (AssertionConsumerService) URL	http://127.0.0.1/wordpress/
Audience URI	http://127.0.0.1/wordpress/wp-content/plugins/miniorange-saml-20-single- sign-on/
NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Recipient URL	http://127.0.0.1/wordpress/
Destination URL	http://127.0.0.1/wordpress/
Default Relay State (Optional)	Available in the <b>premium</b> version
Certificate (Optional)	Available in the <b>premium</b> version

🔞 📸 wordpress 📀	1 🛡 0 🕂 新建	
🚳 仪表盘	常规选项	
★ 文章 9) 媒体	站点标题	wordpress
□ ■ 页面 ■ 评论	副标题	又一个WordPress站点 用简洁的文字描述本站点。
<ul> <li>▶ 外观</li> <li>▶ 插件 1</li> </ul>	WordPress地址 ( URL )	http://127.0.0.1/wordpress
🛓 用户	站点地址(URL)	http://127.0.0.1/wordpress
□ 设置 常規 撰写	管理邮件地址	THE CALL SELECTION THE THOUTING SECTION , IFTEN AVAILATION , INCLUDING AVAILAT
阅读 讨论 想体	成员资格	○ 任何人都可以注册
原本 固定链接 隐私	新用户默认角色	[订阅者 ~]
iminiOrange SAML 2.0 SSO	站点语言 📭	(简体中文 ~ )
收起菜单	时区	*上海         >           洗沒与你左肩—射汉的城市动—へ川了((协调世現社))时汉偏終
今日优选 ≥ <u>70岁老中</u>	医!治疗肝病 , 不能错过这个好方法	! ご問

2. miniOrange若不允许修改配置,原因是用户没有登录miniOrange,点击下图红框中的超链接进行登录。

		alhost/wordpress/wp-admin/admin.php?page=me	_saml_settings&tab=config	
	🛄 应用 🌗 在线JSON校翻	論指式化 🗋 EndUser Portal API ( 🔤 JSON在线解析及槽:	🔍 企业微信 📃 九州云腾	
	🚯 者 test 🛡 0 🕂	新建		磷,
	4월 仪表盘	(Warning: PHP openssl extension is not installed or disab	ed)	
	★ 文章	Account Setup Identity Provider Service	Provider Attribute/Role Mapping Help & FAQ Licensing P	ans
	9]娱体			Support
	📕 页面	Please Register or Login with miniOrange to configu	re the miniOrange SAML Plugin.	Need any help? We can help you with configuring your identity i
	♥ 评论	Step 1:		Just send us a query and we will get back to you soon.
	🎓 外观	You will need the following information to configur	your IdP. Copy it and keep it handy:	Enter your email
	▶ 插件			■ ▼ +1
(	▲ 用户	SP-EntityID / Issuer	http://localhost/wordpress/wp-content/plugins/miniorange-saml-20-si sign-on/	Write your query here
•	≁ ⊥具	ACS (AssertionConsumerService) URL	http://localhost/wordpress/	
	□ 设置 ○ miniOrange SAML	Audience URI	http://localhost/wordpress/wp-content/plugins/miniorange-saml-20-si sign-on/	ngle- 提交
	<ul> <li>2.0 330</li> <li>◆ 收起菜单</li> </ul>	NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress	
		Recipient URL	http://localhost/wordpress/	
		Destination URL	http://localhost/wordpress/	
		Default Relay State (Optional)	http://localhost/wordpress/	
		Certificate (Optional)	Download (Register to download the certificate)	激活 Windows 转到"设置"以激活 Windows

# 1.9. Jumpserver对接-CAS协议

# 原理和协议

从结构上看, CAS 包含两个部分: CAS Server 和 CAS Client 。 CAS Server 需要独立部署, 主要负责对用 户的认证工作; CAS Client 负责处理对客户端受保护资源的访问请求, 需要登录时, 重定向到 CAS Server。

下图是标准 CAS 基本的请求过程:



CAS Client 与受保护的客户端应用部署在一起,以 Filter 方式保护受保护的资源。对于访问受保护资源的每 个 Web 请求, CAS Client 会分析该请求的 Http 请求中是否包含 Service Ticket。如果没有,则说明当前用 户尚未登录,于是将请求重定向到指定好的 CAS Server 登录地址,并传递 Service (也就是要访问的目的资 源地址),以便登录成功过后转回该地址。

用户在上图流程中的**第 3 步**输入认证信息,如果登录成功,CAS Server 随机产生一个相当长度、唯一、不可伪造的 Service Ticket,并缓存以待将来验证。之后系统自动重定向到 Service 所在地址,并为客户端浏览 器设置一个 Ticket Granted Cookie (TGC),CAS Client 在拿到 Service 和新产生的 Ticket 过后,在第 5,6 步中与 CAS Server 进行身份核实,以确保 Service Ticket 的合法性。

在 IDaaS 中, CAS (标准)应用模板实现了标准的 CAS 流程。它充当一个 CAS Server的角色。当 CAS Cient 决定使用IDaaS作为 CAS Server 时。在登录认证时需要使用 IDaaS 系统中公司的主账号,密码进行认证。

#### 操作步骤

说明 CAS 标准应用目前只能由 Π 管理员 在应用添加菜单中添加,下面是 Π 管理员的应用添加流程配置说明。

1. 以IT管理员身份登录 IDaaS,点击添加应用。找到 CAS(标准),点击添加应用

(一) 阿 概览 快速入门	里云	☆页面6     应用分为     供定制化	33含了所有已支持的可添加应 5两种:一种是支持标准的 J V模板进行对接。	〇 用列表,管理员可以选择需要 WT、CAS、SAML 等模板的的	学家 使用的应用进行初始化配置,并开始后续使用。 2月,在这里可以通过添加对应的称准应用模板来实现单点登录功解	<b>费用 ]</b> 8; 另一种是5	E单 备案 E制应用,本	企业 类应用已经	支持与服务	D Q 点登录或用户	♀ ( 帮助 同步的接口,	2 简体中: 文档 X 由 IDaaS 为师	x 🔮
应用	^	请输入应用名称			Q								
巡用列表		应用图标	应用名称	标签	描述				应用类型	l.		操作	
账户 机构及组	^	[-]	阿里云RAM·用户SSO	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 创建RAM子账户, IDaaS账户和RAM子账户通过映射实现单点登	目该模板,需要 录到RAM。	要在RAM中头	每个用户的	3独 Web应用	3		添加应用	
账户管理		[-]	阿里云RAM-角色SSO	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 需要为每个用户单独创建RAM子账户,IDaaS账户和RAM角色通	l该模板,需l 过映射实现单	要RAM中创建 1点登录到RA	IRAM角色, M。	不 Web应用	3		添加应用	
5 突着难	^	ōs	C/S程序	CS, PC, OIDC	唤醒程序后通过OIDC协议向其传递参数实现登录,适用于可以排	変收解析OID0	C协议参数的	应用。	PC客户	<b>8</b>		添加应用	
认证源 RADIUS		Cas	CAS(标准)	SSO, CAS	CAS(Central Authentication Service,集中式认证服务,版本 2 录协议。在集成客户端和服务訿之间网络通畅的情况下广泛在企 点。	0) 是一种基 全业中使用,者	于挑战、应领 F集成简便,	部的开源单/ 扩展性强的	点登 优 Web应用	1, 移动应用		添加应用	
证书管理 1980	^	J	JWT	SSO, JWT	JWT (JSON Web Token) 是在网络应用环境声明的一种基于 JS 分布式站点的单点登录 (SSO)。JWT 单点登录基于非对称加	SON 的开放椅 密,由 IDaaS	iù佳。IDaaS 将用户状态	使用 JWT 沪 和信息使用	封行 私 Web应用	1, 移动应用, F	°C客户端	添加应用	

2. 配置CAS 应用CAS Client 也就是业务系统需要提供的两个参数:

**ServiceNames:** CAS客户端发起认证的URL地址,一般使用固定格式: jumpserver登录地址 +/core/auth/cas/login/?next=%2F

Target Url: IDaaS发起单点登录地址一般格式为: jumpserver登录地址+/core/auth/cas/login/

#### 账户关联方式:根据实际情况选择,请查看主子账户介绍。

	-	3 工作台			Q 搜	上,	费用 工单 ICP 备案 企业 支持 App 🖸 🛕 🙀 🕥 简体
概览		添加应用				添加应用 (CAS	\$(标准)) ×
快速入门		全部 标准协议	定制模板				图片大小不超过1MB
应用	^ -					应用ID	idaas-cn-7mz295a3501plugin_cas_apereo
应用列表 添加应用		添加应			755 Aut (11 A/A cho (11 ) 16 / A11 A /A	* 应用名称	CAS(标准)
账户 机构及组	^	本 成 加 尼 加 日 の 分 プ IDaaS プ	900了所有已受持的可添加。 的两种:一种是支持标准的 为其提供定制化模板进行对抗	U用列表,管理员可以选择需引 JWT、CAS、SAML 等模板的 g。	要使用的放用进行初始 的应用,在这里可以通道	* 应用类型	☑ Web应用 □移动应用 Web应用只会在用户Web使用环境中显示,"移动应用只会在用户客户端中显示,如果想在多个环境 也和可示使用eWeb速率介
账户管理 分类管理		cas				* ServerNames	https://jumpserver.com/core/auth/cas/login/?next=%2F
认证 认证源 RADIUS	^		应用名称 CAS(标准)	M∰ID plugin_cas_apereo	标器 SSO, CAS		////////////////////////////////////
授权	^					* TargetUrl	https://jumpserver.com/core/auth/cas/login/ IDaaS 发起单点感染时的地址,需要可明具体地址,比例:http://www.abc.com/index
权限系统 应用授权						* 账户关联方式	一 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)
审计 Herberge	×						2017日213 (1999年19月1日) - 1999年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1日1日1
<b>兴日日</b> 相							

3. 点开应用详情,复制 CAS Server URL Prefix参数以便接下来修改 JumpServer 配置文件时使用。



#### 单点登录配置·最佳实践

#### 应用身份服务

三()阿里云	6	✿ 工作台		Q	搜索	费用 工单 ICP 备案 企业 支持 App 🔄 🛕 📜 🕜 简体
概览		应用列表			应用详情 (CA	AS(标准))
快速入门 应用 。	^	Ŵ	应用列表 管理员可以在当前页面管理已经添加的所有应用	1、应用可以实现单点登录和数据同步	TargetUrl	https://jumpserver.com/core/auth/casilogin/ IDaaS 发起单点错误时的地址。 https://thisiteteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteeneeteenee
添加应用 账户	^	添加应用	■約加号和平用品, M1K0和从12月8日于局中状态, 請給入应用名称			Arman Andread Schlaugin_cas_appreologin CAS 客户端认证配置的登录地址,一般配置在客户编登录的拦截器(AuthenticationFilter)中。
机构及组 账户管理 分类管理		应用图标	<u>应用名称</u>	放用ID	CAS Logout URL	https://www.apace.com/enduser/ap/lcation/plugin_cas_apereof.ic.com/ かいいかgin_cas_apereologout CAS 客户端认证配面的受出地址。一般配面在客户端受出的出版器(SingleSignOutFilter)中。
认证 · · · · · · · · · · · · · · · · · · ·	^	应用	(6ve)	/m <sup>1</sup> 1111 1 <sup>1</sup> 12m_cas_apere 认证信息	CAS Server URL Prefix	https://tri: اِنْ الْمَرْنَانَ الْمَرْنَانِ اللَّهُ اللَّهُ اللَّهُ اللَّهُ اللَّهُ اللَّهُ اللَّهُ اللَّهُ ال اللَّهُ الْمَكِنَّمُ اللَّهُ اللَّهُ اللَّهُ اللَّهُ عَلَيْهُمُ اللَّهُ عَلَيْهُمُ اللَّهُ اللَّهُ عَلَيْهُمُ ال
RADIUS 证书管理 授权 ·	~	应用			CAS validation URL Prefix	CAS 查户编认记地址前提,查户编设录、登出等 URL 都在此基础上进行讲说。 https://t=i_@+ta-c-i_@-《}
权限系统 应用授权 审计 、	~	授权	信息	SP及腔地址"	账户关联方式	CAS 客户碳校验 ticket 的地址的层,一般配置在客户端校验 ticket 的拦截器(TicketValidationFilter)中, 账户关联
其它管理●	~					

3. 修改jumpserver配置文件

##是否启用CAS认证 AUTH\_CAS=True ##CAS客户端认证地址 对应之前复制的CAS Server URL Prefix参数 CAS\_SERVER\_URL=https://xxxxxx.login.aliyunidaas.com/enduser/api/application/plugin\_cas\_apereo/xxxxxxxxx

##Jumpserver登录地址 CAS\_ROOT\_PROXIED\_AS=https://jumpserver.com ##要使用的CAS协议版本 CAS\_VERSION=3

5.主子账户绑定,详情可参考主子账户介绍。

完成以上步骤,就可以使用CAS协议单点登录到Jumpserver.

# 1.10. IDaaS对接Figma实践

本文是Figma对接文档,配置SAMLSSO进行单点登录。

### 一、获取Figma中SAML SSO元数据信息

管理员登录Figma控制台, 左侧菜单选择 "Admin settings", 右侧展示区选择 "Settings"

A DECK A READER.	4	Dashboard Teams Members Activity	Billing Resources Settings	
) Search				
B Recent		Settings		
Community	Beta	Settings		
Teambition			Organization profile	Organ
🕈 Admin settings				Add o
Drafts	+			
			Domains	Add a
Shared projects				
SuperHard				1.012
99233			Login and provisioning	Chan
-				SAM
<ul> <li>Anishin A</li> </ul>				Enab
Teambition Desig				SCIM
a reambroon pesig				Enab
whether .				
			Other	Publi
				Enabl

### 在 "Login and provisioning" 部分中,选择 "SMAL SSO"

Dashboard Teams Members Activity Billing Resources Settings

#### Settings

Organization profile	Organization handle Add or change your organization's public profile handle	>
Domains	Add a domain to your organization Allow users from an additional domain to become members of your organization Current domain(s): alibaba-inc.com	Contact support
Login and provisioning	Authentication Change how users log in and authenticate to Figma	Any method 🔰
	SAML SSO Enable and configure SAML SSO for your organization	Enabled >
	SCIM Provisioning Enable and configure SCIM for your organization	Disabled >
Other	Public link sharing Enable users to share links to Figma users outside of your organization	Θ
	Approved plugins Enable the approved list to manage plugin usage	Φ

获取"SP entity ID"和"SP ACS URL",供IDaaS配置SMAL应用时使用
ttings					U Teambit
Or	Irganization profile	Organization handle Add or change your organization's public profile handle		>	
De	SAML SSO		× our organization	Contact support	
	SAML single provider (IdP)	sign-on allows you to manage your users with a third-party identity . For more information, view this help article.			
	like to add an	885x1x2,1x51x1x1x Copy		Enabled	
	SP entity ID SP ACS URL	https://www.figma.com/sami/885.0% @ % @ #000000000000000000000000000000		Disabled >	
0	IdP IdP entity ID	Other Idaas			
	IdP SSO URL	eq:https://statestation/pluginstati	ization	8	
		Edit configuration			
		Show more			

# 二、IDaas中配置Figma的元数据信息

# 2.1、添加SAML应用

以IT管理员登录云盾IDaaS管理平台,点击左侧导航栏**应用 > 添加应用** 在右侧选择一个SAML应用,点击添 加应用。

C)		源加	应用 見わた75をロネはか可まれた!			t HILLMARM		
ン用列表	^	▲ 400	area J m 和 Cochao Malaisi 分为两种:一种是支持标准的 Ji	WT、CAS、SAML 等機板的目	1996319299319991999199404444 2月,在这里可以通过添加	1、7777ANINATOPEL。 打击的东西点用模板中实现整点整要功能,另一种重型和应用,本类点用已经提供了对接种单点整要成用户同步的接口,由 (DaaS 为种植用型种化搅板已 打击的东西点用模板中实现单点要改能,另一种重型和应用,本类点用已经提供了对接种单点整要成用户同步的接口,由 (DaaS 为种植用型种化搅板已	行对援。	
加应用		请输入应用名称				Q		
the Third	^	应用图标	应用名称	应用ID	标签	描述	应用类型	操作
→管理		S	SAML	plugin_saml	SSO, SAML	SAM、(Bacuth Assention Marings Language、安全部面形已通常、新本2.0) 基于 XAM、(协议、使用物点制度(Assention) 的安全全线,石田校 方(Duads)和G國方(位用)之同种連絡合信息。实现最于同胞性物的原色理思、SAM、协议通道期的从证例说,在国内外的公明石和低格石中 有11%(产品20月	Web应用	添加应用
	^	-	Salesforce	plugin_salesforce	SSO	Salesforce 最在世界范围内广泛使用的公有云 CRM 平台(Customer Relationship Management,着户共高管理系统)。它为企业提供了事例管理、任务管理、等件的态件级等笔动的考虑能力,DaaS 实场通过 SMML 协议集成登录员 Salesforce 网站。	Web应用	添加应用
DIUS		O.	OAuth2	plugin_oauth2	OAuth2	OAum 是一个开放的资源接份协议,应用可以通过 OAum 获取到全積 access_token,并携带令镜单超势装造求用户资源,应用可以使用 OAum 应 用模拟年实现统一最合管理。	Web应用	源加应用
管理	^	sts	JWT STS(附网关保护)	plugin_iwt_sts	STS, JWT	WIT STG. 3256RASHP, EXEMPT-9652LWIT	Web应用	源加应用
系统  授权		J	TWL	plugin_iwt	SSO, JWT	JVT(SON Web Token)是正符構造的研究構成的研究構成的一种展子 JSON 的开始形象。[Das5 使用 JVT 进行分布式起动的筹点整要(SSO)。JVT 集合整要整子与对称如果,由 (Das5 将用へ线芯和温度使用站的如果,伸激也应用后,应用使用公明解离并进行设法,使用连属6 第二注,集成简 集。	Web应用, 移动应用, PC客户请	添加应用
	~	Cas	CAS(15011)	plugin_cas_apereo	SSO, CAS	CAS(Central Authentication Service,集中成认证服务,版本 2 0) 是一种基于优战,应要的开源单点重要协议。在集成每个确和服务确定间网络 通畅的情况下广泛在全年传用,有集成限促,扩展性限的优点。	Web应用, 移动应用	添加应用
	~		C/S程序	plugin_cs_oidc	CS, PC, OIDC	論羅信手伝達はOIDCが必須其後連手数实現登录、通用子可以連約將行OIDCが必要認的应用。	PC客户调	源加应用
		6	API网关假护	plugin_oauth2_sts	STS, id_token	使用d_baken中接通过用关以证,更持OAuth2t的议	数据同步	添加应用
		0	2FA园关程的	plugin_application_2fact	2FA层关保約_JWT	幕空所自己のはび方式	Web印刷	(高和の中間)

点击添加SigningKey按钮,输入名称等信息,系统会据此生成应用的证书,私钥保留在IDaaS,公钥导出到SP,用于IDaaS与SP应用通信的签名验签。

导入SigningKey	添加SigningKey		
别名	序列号	有效期	秘钥算法
	10	无数据	

如果没有现成的证书可以选择,则填写以下信息生成一个,其中的名称信息最好是和这个应用比如Figma关联的,方便将来识别。

# 添加SigningKey

*名称	请输入名称
部门名称	请输入部门名称
公司名称	请输入公司名称
*国家	请选择
* 省份	请输入省份
城市	请输入城市
*证书长度	请选择
* 有效期	请选择
	提交取消

### 无论是选择已有的还是刚添加的,找到对应的SigningKey,点击"选择"按钮。

导入SigningKey 添加SigningKey					
别名	序列号	有效期	秘钥算法	算法长度	操作
CN=试用公司, JII-JII, C=CN	1037460220 厚5零;尾头	365	RSA	2048	选择 导出

接下来要填写更多的应用信息,名称等信息可以自定义,SP Entity ID、SP ACS URL(SSO Location)等信息从"一、获取Figma中SAML SSO元数据"中复制过来。

图标	SAML
	◎上传文件
	图片大小不超过1MB
应用ID	idaas-cn-beijing-foyeyjskkp7plugin_saml2
*应用名称	SAML
* IDP IdentityId	
	IDP IdentityId is required
* SP Entity ID	
	SP Entity ID is required
* SP ACS URL(SSO Location)	请输入SP ACS URL(SSO Location)
* NameldFormat	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
* Binding	POST
SP 登出地址	请输入SP 登出地址
Assertion Attribute	Assertion Attribute key - +
	断言属性。设值后,会将值放入SAML断言中。名称为自定义名称,值为账户的属性值。
Sign Assertion	
IDaaS发起登录地	IDaaS发起登录地址
址	以 http://、https:// 开头, 填写后使用 IDaaS 发起登录将会跳转到该地址, 而不会使用 SAML 的idp发起登录流程
*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

### 需要填写的主要信息如下:

参数名称	说明
应用名称	所添加应用的名称,可以为任意值,但最好和应用相关。
IDP IdentityId	在IDaaS中设置的认证参数,需要将此参数配置到SP中, 可设置为: <b>idaas</b>
SP Entity ID	在SP中设置的Entity ID,需要复制到IDaaS的配置中, 可 以在Figma的SMAL SSO中获取
SP ACS URL (SSO Location)	单点登录地址,需要复制到IDaaS的配置中, 可以在 Figma的SMAL SSO中获取

NameldFormat	名称标识格式类型,这里以Figma为例 urn:oasis:names:tc:SAML:1.1:nameid- format:emailAddress
Binding	默认POST方式发送消息到阿里云控制台

填写完成后提交保存,如果应用是禁用状态,可以继续修改重新提交。

# 2.2、启用应用并且授权

应用配置好以后需要先启用应用,并且将服务授权给一个账户,点击左侧导航栏 **应用 > 应用列表** 启用该应 用并授权给账户。

КВ         АЛЯВ           VELO	☰ (-) 阿里	E				Q IERXH, IS	制台、API、解决方面和密查	務用 工单 餐案	企业 支持	章 宣河	۵ ¢	Ħ	⑦ 简体
10207       10207 <th< th=""><th>概范</th><th></th><th>应用列表</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></th<>	概范		应用列表										
Ref         A         All Section         All Section	快速入门 (四用) (四用列表) 添加应用	î	Ŵ	应用列表 管理员可以在当前页面管理已经添加的所有。 当添加完定用后,应该确认应用处于应用状	立用,立用可以实现 <b>单点登录记数据用</b> 卓能力。 5、并已起地成了接权,在应用排嘴中,可以避到应用的冲磁信息,单点登录地站。	子账户配置、同步配置、授权、审计等信息							
1月以近 角川間毎 白用名本 白用D 设备类型 白用状态 二次从证状态 操作	账户	^	添加应用	清输入应用名称		Q							
	利用以因		应用图标	应用名称	应用ID	设备类型	应用状态	二次认	正状态		10	ft	
3 英語语 SAAA. forma idaas-cr-beijing-frysjologi/gaugit_samit Web应用 💽 🕥 IBC 17月 -	分类管理		S	SAML-figma	idaas-cn-beijing-foyeyjskkp7plugin_saml1	Web应用					援权	胡 -	

### IDaaS支持多种方式进行授权,这里以按应用授权账户为例。

≡ c-)®	里云			Q 搜索文档、控制台、API、解决方案和资源
概范 快速入门		应用授权 应用授权主体 主体授权应用		
应用 应用列表 添加应用	^	<u></u>	<u>廃た</u> 福 福岡町(均 分開	
账户 机构及组 账户管理	^	SAML-figma Q SAML-figma >	第編入第六名称出行意比 ■ 自身報子的反現支援 ◎ 拒绝自身報子的反現支援 ◎ 能承 (編、編) ■ 報告名曲	(21)构、分类) 赋予的权限资源 📑 继承拒绝(道 思元名政
万突管理 认证 认证源	^	共1条 < 1 >	ingtao.]p	

保存后,这个用户登录就可以看到这个应用了。

# 2.3、IDaaS关联子账户

一个系统要SSO到另外一个系统,需要使用对方能够识别的子账号进行认证,往往登录到IDaaS的主账户和应用SP的子账户是不一样的,可以使用账号同步(两套系统中的账号信息相同)或者新建子账户进行账号映射的方法。账号映射是指给IDP的账户建立一个SP中已经存在的账户作为子账户,身份认证的时候通过子账户进行认证。例如SP系统中有个账户"test@alibaba-inc.com",我们想用IDP系统中的"test.sp"账号SSO到SP,则需要给账号"test.sp"新建一个对应的子账户"test@alibaba-inc.com"。这里以Figma演示新建子账户的功能,如下图,Figma中有账户test@alibaba-inc.com。

00	Search Recent Community	Beta	Members					Teambition
0	Teambition		Account type: All ~ Role: All ~ Last edit: All ~	New since last invoice		Q.)	Invite	users 🛓 Request full CSV
\$1 •	Admin settings Drafts	+	□ Name ↓	Last edit	Last active	Date upgraded	Role	
88	Shared projects		(You) Admin	14 days ago	5 hours ago	Dec 28, 2020 ④	Editor ~	
	SuperHard		Palibaba-inc.com	1 - I	2 hours ago	-	Viewer ~	
•	PPTPP.							
	é nigiska							
	Teambition Desig	gn						
•								

IDaaS中新建子账户有两种方式,操作如下:

# 2.3.1、普通账户申请关联子账户

普通用户登录,点击左侧导航栏 **主导航 > 应用子账户** 添加应用子账户功能中提交新建子账户申请。由于上 一步Figma账户是jingtao.ljt@alibaba-inc.com,所以这里子账户的名称应该填 "jingtao.ljt@alibabainc.com"。

IDaaS统一认证身份平台				添加子账户	
欢迎 · IDaa S	应用子账户				
				选择应用	SAML-figma
1940	子账户列表 子账户审批				请选择关联的应用
首页 应用管理				主账号	ji gao a
(应用子账户)	79488/2019 3 74N *		4		
設置 ^	应用的标 应用名称	<b>审批状态</b>	主張戶	子账号	ingen: ingalibaba-inc.com
我的账户			誓无欺握		權示: 此应用于账户采用的是 <b>账户关联</b> 方式,您需要提供正确的用户名才
二次认证表的消息					Ote Pro-
我的日志					UK 67 ALCHI

登录管理员账户,点击左侧导航栏 其它管理 > 审批中心 审核通过该应用子账户的添加。

≡ e	)阿里云						Q 建汞文档、控制台、	API、解决方案和资源	鹿用 工	¥ 92	企业	支持	實河 区	۵. ۵	7 C	简体
概范		审批中心 VIP														<b>WILL</b>
快速入门		子账户审批 注册审批 应用审批														
应用 账户 认证 授权 案は	* * * *	★ 設中心 一部市小温 Daas 系统中管理员集中处 子联小和印度单必是很可能会可能会 事批通过机用户将可以使用子托小单、	理所有需要审批内容的功能页面。当有代 分标记,如果某应用设置其主子所冲映射 企业是到应用系统中,请确认 (DaaS 用户	等事批项出现时,会在左侧 关系为[账户关联]时, 户主账户和子账户的对应关	导航栏相应位置有数寸 用户在尝试单点登录的 ) 風后完成审批。	P气泡熄示。 时候,如果没有子账户	9,则会继交一个子账户继定	申请。由管理员在此处送	行审批。							
展它管理	<b>`</b>	主账户 (申请人) 子账户	应用名称	待审批 〜	9. 数数	<b>重要</b> 当前审批如	國自用外部审批流,请到外	部审批平台进行处理!								
家族中心	> •	主账户 (申请人)	子账户	应用名	10×10		申请时间		审批状态				12	PE .		
消息管理		log-he al	inin a galbaba-inc.com	SAML	-figma		2020-12-29 18:42:57		将审批				-	<b>香洋情</b> 快速	同意 快速	60 ¥2
会话管理 我的消息 20季	•												共1条	< 1	> 14	至 1

# 2.3.2、管理员关联子账户

管理员新建子账户不需要审核过程,具体操作为:

登录管理员账户,点击左侧导航栏 应用 > 应用列表 找到添加的应用,点击详情中的查看应用子账户。

E G	阿里云						Q 搜索文档、控制台、API、解决方案和附置	興用 工单	發賞	企业	支持	官同	E .	р. А	0
概波		应用列表													
快速入口 使用 应用列表 添加应用	^	© 管理 当派	<b>明列表</b> 医页可以在当前页面管理已经添加的所有应用。 加加应用后,应该确认应用处于应用状态,非	应用可以实现 <b>单点</b> #已经完成了版权。そ	登景和数据明华能力。 12月19년年,可以看到应用的详细信息、单点登录地址	止、子账户配置、同步配	<b>眉、投权、审计邻信息。</b>								
账户	~	添加应用	请输入应用名称			Q									
认证	Ŷ	应用图标	应用名称		应用ID	设备类型	应用状	8	二次认识	EKS				现作	
审计	*	S	SAML-figma		idaas-cn-beijing-foyeyjskkp7plugin_saml1	Web应用	C	)					援权	洋街 🔺	
其它管理	~														
设置	×	应用信息			认证信息		账户信息 - 同步		9	白信息・う	P账户				
		应用的详			应用的单点登录地址		SCIM协议设置以及把组织机构、组同步推进至应用		4	6主账户:	与应用系统	中子账户	的关联表		
		宣君详情	修改应用 删除应用		IDaaS发起地址		同步机构 SCIM配置		2	看应用子	8A				
		授权信息			审计信息		API			課应用内核	双限				
		应用与人	员组织的摄权关系		查看应用系统详细的操作日志		是否对应用开放系统API		1	现应用内	東单与功能	的限			
		授权			査署日本 査署同歩记录		API Key API Secret		9	定权限系统	Ŕ				

### 点击添加账户关联,添加子账户。

E (-))	何里云	Q RERCH. HING. AP. MARSERRER RE IN SEC 20 RE EN () TO ()	0
概述		应用列表 / <b>7第户</b>	
快速入门		← 子账户	
<u></u> <u></u>	ž	子教户 予教・知識最互相定意用系統中、用小会に什么最会进行活用、主席小型的環 Das5 中的原介、石田行用の設置材、Das5 合作信用系統件運行信約子符合、協子指小型要互合用系統中存在且可问题。 部列、Das5 中有互換小 除三(用小名 changum)、正全出的 BFM 信用系統中、这个用小型用小名量 appodman、与互換小 Anargam 进行关键。 限小类的方式、在应用地罐材、软果选择了整小标材、影像以主要小标子将小类点一起、天果配置、如果选择了加小关键、制能要在注意进行手续的分子很小心理和上子将小关键。	
授权 审计 其它管理	\$ \$ \$	SAML-figma	

输入授权账户(主账户)和子账户,点击保存完成子账户添加。

主账户:登录IDaaS使用账户。

子账户: SP应用中的子账户

# 三、Figma中配置IDaaS的元数据信息

# 3.1、获取IDaaS的元数据信息

以Ⅱ管理员账号登录云盾IDaaS管理平台,点击左侧导航栏**应用 > 应用列表**选择刚才添加的应用,点击查看 详情,如下图:

≡ ⊖ 🕅	里云					Q 撤退总统, 经制化, API, 解决方面和	第二章 第月	IM	發度	企业 支持	官同	5.	۵.	₹ (1)	10
概况		应用列表													
供速入门 (定用) (定用列表) 液加应用	î	应用歹 管理员 当添加	9要 可以在当朝京憲管理已給添加的所有应用。应用可以定取 <b>中</b> 売应用后,应该确认应用社子目用状态,并已经完成了授权。	全 <b>争承征教师时</b> 并能力。 在应用评值中,可以看到应用的评细信息,单点登录地址, <sup>1</sup>	子账户配置。同步配	還、 授权、 审计等信息。									
账户	2	海和麻用	输入应用名称		٩										
认证	×	应用图标	应用名称	应用ID	设备类型		应用状态		二次认证权	ø			跟作		
接权审计	> >	S	SAML-figma	idaas-cn-beljing-foyeyjskkp7plugin_saml1	Web应用							授約	x (##	•	
其它管理	×														
设置	×	应用信息		认证信息		账户信息 - 同步			账户	自己 · 子账户					
		应用的详细(	18	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	甚至应用		平台	主账户与应用)	(统中子师)	~ 的关联	R.		
		查看洋街	修改应用 删除应用	IDaaS波起地社		同步机构 SCIM配置			皇君	应用子账户					
		緩权信息		审计信息		API			10100	拉用内权限					
		应用与人员的	目的的授权关系	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》	②用内菜单与3	加密权规				

点击导出SAML元配置文件,将IDaaS的元数据文件保存到本地电脑。

图标	SAML
应用ID	idaas-cn-beijing-foyeyjskkp7plugin_saml1
应用名称	SAML-figma
应用Uuid	c5ae04c3c9f02a4c6ec148f3257cc276TMxbr0aHFpS
SigningKey	191 <del>3</del> 09 38 1916333 (066 (CN=SAML)
NameIdFormat	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
SP ACS URL	https://www.figma.com/saml/9HEPHEESSINESSINESSINESSINESSI
IDP IdentityId	idaa: 导出 IDaaS SAML 元配置文件
SP Entity ID	https://www.figma.com/saml/88ED Int toos Interest 676
Binding	POST

## IDaaS元配置文件示例如下:

1	[] <md:entitydescriptor entityid="idaas" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"></md:entitydescriptor>
2	<pre>cmd:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"&gt;</pre>
3	<pre>d<md:keydescriptor use="signing"></md:keydescriptor></pre>
4	<pre>cls:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"&gt;</pre>
5	e <ds:x509data></ds:x509data>
6	<ds:x509certificate></ds:x509certificate>
	MIIB9zCCAWCgAwIBAgIIGpblwuj49s4wDQYJKoZIhvcNAQEFBQAwPjELMAkGA1UEBhMCQ04xDzANBgNVBAgMBuaxn+iLjzEPMA0GA1UEBwwG5Y2X5LqsMQ0wCwYDVQQDEwRTQU1MMB
	MAKGA1UEBhMCQ04xDzANBgNVBAgMBuaxn+iLjzEPMA0GA1UEBwwG5Y2X5LqsMQ0wCwYDVQQDEwRTQU1MMIGfMA0GCSqGsIb3DQEBAQUAA4GNADCBiQKBgQCY5IaMlj0e2AsN73hEfz
	vs+VbTRZuQ0Lo3tF16S70DsVEe77CbrsMFdidFAbDyn5r1D1isoo4H5ifwTxKTQ9Lc49D80B3j5XsfiKt20Parts/fdqcL9yAmDoa0IDAQABMA0marts/SIb3DQEBBQUAA4GBAI
	aZYUNQD30RBZcoxkZuGiphcxShW04SDB/T4rnXVS1Y0daeswn34u5fyWeR5zfL1Pg3S/
7	-
8	-
9	-
10	<pre>d<md:keydescriptor use="encryption"></md:keydescriptor></pre>
11	e <ds:keyinfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"></ds:keyinfo>
12	e <ds:x509data></ds:x509data>
13	<ds:x509certificate></ds:x509certificate>
	MIIB9zCCAWCgAwIBAgIIGpblwuj49s4wDQYJKoZIhvcNAQEFBQAwPjELMAkGA1UEBhMCQ04xDzANBgNVBAgMBuaxn+iLjzEPMA0GA1UEBwwG5Y2X5LqsMQ0wCwYDVQQDEwRTQU1MMB
	MAKGA1UEBhMCQ04xDzANBgNVBAgMBuaxn+iLjzEPMA0GA1UEBwwG5Y2X5LqsMQ0wCwYDVQQDEwRTQU1MMIGfMA0GCSqGSID3n_MBAQUAA4GNADCBiQKBgQCY5IaMlj0e2AsN73hEfz
	vS+VbTRZuQ0Lo3tF16S70DsVEe77CbrsMFdidFAbDYn5r1D1iSoo4H5ifwTxKTQ9Lo49D80B3j5XsfiKt20Pc1vzb2866mmc19mmc19mmc19mmc19mmc19mmc19mmc19mmc
	aZYUNOD30RBZcoxkZuGiphcxShW04SDB/T4rnXVS1Y0daeswn34u5fyWeR5zfL1Pg3S/U+2J1JyP0
14	
15	
16	-
17	<pre><md:singlesignonservice_binding="urn:oasis:names:tc:saml:2.0:bindings:http-redirect"_location=< pre=""></md:singlesignonservice_binding="urn:oasis:names:tc:saml:2.0:bindings:http-redirect"_location=<></pre>
	"https://mpluluiumb.login.aliyunidaas.com/enduser/apj/application/plugin_saml/idaas-cn-beijing-foyerplugin_saml1/sp_sso"/>
18	<pre><md:singlesignonservice binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" location="&lt;/pre"></md:singlesignonservice></pre>
	"https://
19	
20	L

获取上图位置Url地址。(Figma配置IdP SSO target URL使用)

导出证书(Figma配置Signing certificate使用):

点击左侧导航栏 应用 > 添加应用 在右侧选择一个SAML应用,点击添加应用。

≡ c	〕阿里云					٩	脱脱文档、拉制台、API、解决方案和	回题 義用 王单 發度 企业	12 交換 112 〇〇	#190 ® #	0
概范 快速入门		添加店 () 本市際	月 9月 - 765月日本時約可透知点5	电利表 普德昂可以连续感	夏後用的点田洋兵が始び配帯	却开始忙碌得田				×	
应用 应用列课	n.	₩ 4500m 应用分:	5回17所有CSC465与60000 为同种:一种是支持标准的 JV	9758、BALLASAALINA	9007603出762710346744篇。 1应用,在这里可以通过添加25	9777 MARANGEONE, 在的标准应用模板未实现单点登录功能:另一种最定制应用。	本與应用已經提供了对接其单点登录或	用户局步的接口,由 IDaaS 为其提供定制化	機振进行対接。		
深加应用 账户		请输入应用名称 应用图标	应用名称	庭用ID	标签	<b>Q</b> 振送			应用类型	提作	
利,构及3 账户管理 公选管理		S	SAML	plugin_saml	SSO, SAML	SAML (Security Assertion Markup Language, 安全新言い 方 (IDaaS) 和消費方 (应用) 之间传递身份信息, 实现道 有非常广泛的运用。	示记语言,版本 2.0)基于 XML 协议,6 行网络跨域的单点登录。SAML 协议是	明相包含新言(Assertion)的安全令律。在 成熟的认证协议,在国内外的公有云和私有	受权 云中 Web应用	添加应用	
认证	^	-	Salesforce	plugin_salesforce	SSO	Salesforce 是在世界范围内广泛使用的公有云 CRM 平台 理。任务管理、事件动态升级等高效的商业能力。IDaaS 3	(Customer Relationship Management, 5時通过 SAML 协议单项登录到 Salesfo	春户关系管理系统),它为企业提供了事例 rce 网站。	馆 Web应用	添加应用	
RADIUS	3	ONTE	OAuth2	plugin_oauth2	OAuth2	OAuth 是一个开放的资源颁权协议,应用可以通过 OAuth 用模板来实现统一身份管理。	获取到令牌 access_token,并携带令牌	来服务诱请求用户资源。应用可以使用 OAi	uth 应 Web应用	添加应用	
近书曾3 授权		sts	JWT STS(附同关保护)	plugin_jwt_sts	STS, JWT	JWT STS, 支持网关保护, 签发JWT与校验JWT			Web应用	添加应用	
权限系统	е 2	J	JWT	plugin_jwt	SSO, JWT	JWT(JSON Web Token)是在网络应用环境声明的一种器 单点登录基于非对称加密。由 IDaaS 将用户状态和信息使 单。	#于 JSON 的开放标准。IDaaS 使用 JW 用私钥加密,传递给应用后,应用使用公	T 进行分布式站点的单点整景 (SSO)。J 3.钥解密并进行验证。使用场最非常广泛,\$	WT 影成简 Web应用, 移动应用, PC客户到	青 添加应用	
审计 其它管理	*	Cest	CAS(标准)	plugin_cas_apereo	SSO, CAS	CAS (Central Authentication Service,集中式认证服务, 通畅的情况下广泛在企业中使用,有集成简便,扩展性强。	版本 2.0)是一种基于挑战、应答的开音 9代点。	種亦聖景协议。在集成客户論和服务論之间	网络Web应用,移动应用	添加应用	
19.M	~	<b>P</b>	C/S程序	plugin_cs_oidc	CS, PC, OIDC	鏡驅程序后還过OIDC协议向其传递参数实现登录,适用于	可以接收解析OIDC协议参数的应用。		PC客户销	添加应用	
添	加应用	] (SAM	L)								×
	导入Sign	ingKey	添加Signin	ngKey							
7	间名			序	初号		有效期	秘钥算法	算法长度	操作	
C	N=SA₩	, - 18 <b>9</b> , 3	I∏ej5, C=CN	1	915971	17.5.66	30	RSA	1024	选择 导出	

在导出SigningKey页面,勾选 "Base64 编码 X.509(.CER)(S)",保存至本地电脑。

确定	取消
----	----

# 3.2、Figma中配置元数据信息

管理员登录Figma控制台, 左侧菜单选择"Admin settings", 右侧展示区选择"Settings", 在"Login and provisioning"部分中,选择"SMAL SSO", 在配置页面点击"Edit configuration", 编辑配置页面, 选择"Other".

identity provider (IdP). For more information on where to find this information, view this help article.

# Identity provider (IdP)

Okta

Microsoft Azure Active Directory

OneLogin

Other

# IdP entity ID

idaas

# IdP SSO target URL

https://mplelnlywb.login.aliyunidaas.com/enduser/api/application/plugin\_sa

# Signing certificate

选择文件 864cb34c84cde...R6WbD (1).cer

	Denter
Cancel	Review

参数	说明
IDP IdentityId	与IDaaS添加应用时IDP ldentityld保持一致,这里 以"idaas"为例
IdP SSO target URL	ldaaS单点登录地址,3.1中获取的元数据信息中的地址
Signing certificate	单点登录的证书,3.1中导入的SigningKey

# 四、功能演示

# 4.1 IDP发起SSO

配置完成后, 就可以检查结果了。授权用户登录IDaaS, 点击左侧导航栏 **主导航 > 首页** 在我的应用中点击 该应用进行单点登录, 点击应用的图标进行单点登录。



首次登录, Figma会要求进行一次账户认证,认证完成后进入登录。(只限首次认证登录)

认证成功后登录Figma,然后就可以看到Figma作为SP提供的资源了。

# 4.2 Figma发起SSO

同样,正确配置后,也支持SP发起,首先找到Figma登录地址,选择"Log in with SAML SSO"。

G Lo	; in with Google	
	or	
Email		
Password		
	Log in	
Log	with SAML SSO	
No. or		

在SAML SSO页面输入Figma账户的邮箱地址

# Log in with SAML SSO

# Log in to Figma with SAML SSO

alibaba-inc.com

Log in

Log in with Google or a password

跳转到IDP进行用户认证,只有IDaaS中添加的账户进行登录

	扫码登录更便建
阿里云	IDAAS
请输入用户名、邮箱、引	印代春
请输入密码	
	忘记密码
₩	录
注	<del>19</del>
第三方:	人证登录
🔵 🖬 🐑	

IDP认证通过后,然后就可以看到Figma提供的资源了。

# 1.11. Salesforce对接

本文为您介绍如何在IDaaS中使用SAML协议单点登录到Salesforce。

# 背景信息

Salesforce是一家创建于1999年的客户关系管理(CRM)软件服务提供商,总部设于美国旧金山,可提供随需应用的客户关系管理平台。Salesforce支持SAML协议实现单点登录,本文将说明如何在IDaaS中使用SAML协议单点登录到Salesforce。

### 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. 在左侧导航栏,点击 应用>添加应用,选择Salesforce应用模板,点击"添加应用"按钮。

欢迎 · IDaaS	请输入应用名称			٩		
概定	应用图标	应用名称	标签		应用类型	操作
★ 应用 应用列表	Cus	CAS(标准)	SSO, CAS	CAS(Central Authentication Service, 集中式认证服务, 版本 2 0) 是一种基于组成,应该的开源单点望录 协议,在集成案件编码服务课名间网络遗植的徽方下广泛在企业中使用,考集成添强,扩展性强的优点,Daa S 平容支持 CAS 标准 和 CAS 改良(开設中) 两种 CAS 单点登录方式, CAS 改良 可以支持和 IOP 发起的单 流登录)。	Web应用, 移动应用	添加应用
添加应用 ^ 用户	J	JWT	SSO, JWT	JWT (JSON Web Token) 是在网络应用环境砷铜的一卷基于 JSON 的开放控集。DaaS 使用 WT 进行分布 式站在的单点登录(SSO),JVT 单点登录基于菲波称如此,用 DaaS 将用产材式和信息使用私相加密,使 递给应用后。应用使用之终期牵开进行验证。使用逐量非常广发、集成原稿。	Web应用, 移动应用, PC客户端	添加应用
账户及组账户管理	OAUTH	OAuth2	OAuth2	OAuth 是一个开放的流環授权协议,应用可以通过 OAuth 哀取到今婢 access_token,并携带今碑未服务训请 求用户资源,应用可以使用 OAuth 应用模板来实现统一身份管理。	Web应用	添加应用
へ 授权 应用授权	SAML	SAML	SSO, SAML	SAML (Security Assertion Martup Language, 安全新售标记面档, 原本 2.0) 基于 XML 协议、使用包含新 音 (Assertion) 的安全令候, 在授权D (Dass) 和词称为(原用) 之间传递得的信息, 实际基于网络原始的 单纯管理。XML 协议是成绩的以证协议, 在国内分约公约支付和代格支付中非常广泛的运用。	Web应用	添加应用
权限系统	salesforce	Salesforce	SSO, SAML, CRM	Salesdore 是在世界范围为广泛使用的公布云 GRM 平台(Customer Relationship Management, 客户关系管 理系统),它为企业提供了事例管理。C好管理、事件动态升级等等高效的弯业能力。iDaaS 支持通过 SAAL 协议用产程展录到 Salesdore 防杀。	Web应用	添加应用
<ul> <li>从止</li> <li>认证源</li> <li>证书管理</li> </ul>	Ŵ	WordPress-SAML	SSO, SAML, CMS	WordPress 是全世界最初广泛使用的 CMS(Content Management System, 内容管理系统), 它通过非常强 大规模相关系统冗仿电放松器件界面, 方许了千万技术或非技术人员生产, 管理各种类型的网站, 从电边网 站, 取符页面型人内爆客, 主题论坛, WordPress 所支持的形式非常多样, IDaaS 支持通过 SAML 协议单点 登录到 WordPress 网站。	Web应用	添加应用
Radius へ 审计		云梦	SSO, JWT, 阿里云	阿里云市场应用厂商 云梦 提供的企业信息化服务应用,基于 JWT 应用模板接入。	Web应用, 移动应用, PC客户端	添加应用

3. 选择一个 SigningKey(如没有,可先添加一个SigningKey),并选择导出,此步骤需要会载一个cer证 书到本地。

励应用(Salesforce)							
导入SigningKey 添加	)]]SigningKey						
Alias	SerialNumber	ValidityDays	KeyAlgorithm	KeySize	操作		
CN=ceshi, L=chengdu, S T=sichuan, C=CN	5746000010103094381	180	RSA	1024	选择 导出		
CN=hello610, ST=四川, C =CN	6827849760824944784	365	RSA	2048	选择 导出		
CN=D, ST=SC, C=CN	9209550121381603185	365	RSA	2048	选择 导出		
CN=ceshi624, ST=四川, C=CN	3184516042212719933	365	RSA	2048	选择 导出		
CN=628, ST=sdfsd, C=C N	5685282424851731004	365	RSA	2048	选择导出		

4. 以管理员帐号登录Salesforce, 点击右上角"设置"按钮。

		*• 🖬 ? 🌣	. 🖡 👩
1.1		<b>坟</b> 设置	0
]理		管理订阅	
· 👻	业务机会包含逾期任务 Acme - 1,200 Widgets (Sample)	Developer Console	×
· 👻	30 天没有任何活动 Global Media - 1750 Widgets (Sample)	编辑页面	ii ×
¥	30 天没有任何活动 salesforce.com - 240 Widgets (Sample)	ž	≡ 🛱 ×

5. 进入设置主页, 找到设置处, 依次点击左侧菜单栏: 身份-单点登录设置, 找到 SAML单点登录设置, 点击"新建"按钮。

and the state of the		
> 对象和字段	☆ 设置 前占容录设置	
> 流程自动	十爪豆水咬目	
> 用户界面	单点登录设置	
> 自定义代码	配置单点登录,以便从外部环境验证 salesforce.c	om 中的用户。您的组织对单点登录有以下可用选项:
> 环境	• 联盟验证是一种使用发送到 Salesforce	满点的 SAML 声明的单点登录方法。
设置		编辑 SAML 声明验证器
> 公司设置	使用 SAML 的联盟单点登录	
~ 身份	SAML已启用	
单点登录设置	SAML 单点登录设置	新建 元数据文件的新增功能 元数据 URL 的新增功能
登录历史	无 SAML 单点登录设置	
身份提供商		
身份验证历史		
验证提供商		
> 安全性		

6. 进入Salesforce SAML单点登录设置页面。

SAML 单点登录设置			
	保存】保存并新建 取消		
姓名	IDaas	API 名称	ceshi
SAML 版本	2.0		
颁发人	https://idp4.idsmanager.com	实体 ID	https://saml.salesforce.com
身份提供商证书	遗择文件 未遗择任何文件	当韵证书	CN=D, ST=SC, C=CN 到期: 23 Jun 2020 07:22:23 GMT
请求签名证书	SelfSignedCert_24Jun2019_064740 V		
请求签名方法	RSA-SHA1 V		
声明解密证书	■明未加密 ▼		
SAML 身份类型	<ul> <li>         ・</li></ul>		
SAML 身份位置	<ul> <li>         ・身份在:主部:声明的 NameIdentifier 元素中         ・         ・         ・</li></ul>		
身份提供商登录 URL			
自定义注销 URL			
自定义错误 URL			
单点注销已启用			

- 姓名: 该SAML单点登录设置名字, 随意输入;
- 颁发人:注意此值应该与下面我们在IDP2中配置Saleforce SAML中IDP Identity Id一致;
- **实体ID**: https://SAML.Salesforce.com;
- 身份提供商证书:选择我们刚刚在IDaaS导出到本地的证书文件;
- 。 请求签名证书: 默认即可;
- 请求签名方法: RSA-SHA1;
- 声明解密证书:选择"声明未加密";
- SAML身份类型:选择"声明包含用户的Salesforce用户名";
- SAML身份位置:选择"身份在"主题"声明的Nameldentifier元素中";
- 身份提供商登录URL,注销URL,自定义错误URL留白即可,点击保存;
- 7. 添加成功,会显示该SAML名称设置的详细信息,注意将Salesfore 登录URL复制出来,以备后用。

SAML 单点登录设置	
	编辑 删除 复制 下载元数据 SAML 声明验证器
姓名	
SAML 版本	2.0
颁发人	https://idp4.idsmanager.com
身份提供商证书	CN=D, ST=SC, C=CN 到期: 23 Jun 2020 07:22:23 GMT
请求签名证书	SelfSignedCert 24Jun2019 064740
请求签名方法	RSA-SHA1
声明解密证书	声明未加密
SAML 身份类型	用户名
SAML 身份位置	主题
身份提供商登录 URL	
自定义注销 URL	
自定义错误 URL	
单点注销已启用	
において、「「「」」」	
端点	
为贵组织、社区或自定义域,查看 SAML 端点。	
您的组织	
登录 URL	https://login.salesforce.com?so=00D2v000001XLmT
OAuth 2.0 标记端点	https://login.salesforce.com/services/oauth2/token?so=00D2v000001XLmT
	编辑 删除 复制 下载元数据 SAML 声明验证器

### 备注,也可点击该SAML设置的名称进入以上页面查看Salesforce 登录 URL

SAML 单点	登录设置	新建	元数据文件的新增功能 元数据 URL 的新增功能	
操作	姓名	SAML 版本	颁发人	
编辑 删除	IDaas	2.0	https://idp4.idsm	nanager.com

8. 找到单点登录设置,联盟验证处,点击"编辑"按钮

单点登录设置					
配置单点登录,以便从外部环境验证 salesforce.com 中的用户。您的组织对单点登录有以下可用选项:					
• 联盟验证是一种使用发送到 Salesforce 端点的 SAML 声明的单点登录方法。					
	编辑 SAML 声明验证器				
使用 SAML 的联盟单点登录					
SAML 已启用					

9. 勾选"SAML已启动", 点击 保存

单点登录设置
--------

	保存	取消
使用 SAML 的联盟单点登录		
SAML 已启用 🛛		
	保存	取消

# 10. 回到IDaaS中添加Salesfore页面,点击"选择"按钮,进入Salesforce的SAML配置页面。

应用ID	wceshisalesforce2
SigningKey	6827849760824944784(CN=hello610)
* 应用名称	Salesforce-勿删
* 所属领域	其它
* 应用类型	✔ Web应用
* IDP IdentityId	https://idp4.idsmanager.com
	IDaaS IdentityId is required
* SP Entity ID	https://saml.salesforce.com
	SP Enuty ID is required
* SP ACS URL(SSO Loc ation)	https://login.salesforce.com?s
SP 登出地址	请输入SP 登出地址
* NameldFormat	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
* SP登录方式	应用自定义登录页 ~
Sign Assertion	No

### 。 IDP Identity Id为在Salesforce填写的颁发人值;

### ○ SP ACS URL(SSO Location)为 Salesforce 登录 URL,为我们在上面复制的Salesforce 登录 URL值;

⑦ 说明 该URL格式为 https://login.Salesforce.com?so=<您的组织ID> 的形式。如果您不确定Salesforce组织ID,请转到Salesforce中的公司简介->公司信息来查找。

### 11. 启用应用并授权

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
salesforce	Salesforce-勿删	wceshisalesforce2	Web应用	$\bigcirc \times$	×	授权 详情 ▼
应用授	2					
按应用授	教组 按组授权应用					
应用(	1)		<b>组 (7002)</b> 已授权 (4个)			
Sales	Salesforce-勿删 提示:授权时,子级组会默认继承父级组的权限,若要单独取消子级组权限,请解除父子级组之间的关系即可。					
Sales	sforce-勿删	>	请输入组名进行搜索			
	共1条 〈	1	□- □ ● 阿里云: DaaS服务 □- ☞ ■ 阿斯顿撒旦			
			王 🕑 🌆 Test接口专用			

### 12. 添加子账户并进行单点登录

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
salesforce	Salesforce-勿删	wceshisalesforce2	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	
应用的详细	暗息 (禁用后可编辑)	应用的单点登录地址		平台主OU/账户对应应用器 表	系统中子OU/账户的关联	应用与人员组织的授权	关系
查看详情	修改应用 删除应用	IDaaS发起地址		查看应用子账户		授权	
审计信息		API					
查看应用系	5统详细的操作日志,确保应用安全	应用对外调用的API接口					
查看日志	查看同步记录	X API Key API Se	ecret				
et en plate	- <b>7</b> 844						
← 子账	沪					添加账户关联	批量导入 批量导出
Salesfor	ce-勿删						
主账户(	账户名)		٩				
主账户	子账户	显示名称    子	账户密码	是否关联	审批状态	关联时间	操作
draven	974301102@qq.com	draven6 无		未关联		2019-06-24	删除

添加账	户关联		×
* 主账户 账户名	(邮箱/手机号/ 称)	主账户 (邮箱/手机号/账户名称)	
* 子账户		子账户	
		<b>保存</b> 返回	
欢迎 · IDaaS	我的应用		
主导航 ^ 首页	Web应用		
<ul> <li>(2)開催機</li> <li>(2)置 ^</li> <li>(2)数 / (2) (3) (4)</li> <li>(3) (4)</li> <li>(3) (4)</li> <li>(4) (4)</li> <li>(4) (4)</li> <li>(5) (4)</li> <li>(5) (4)</li> <li>(5) (4)</li> <li>(6) (4)</li> <li>(7) (4</li></ul>	CG_applications	UTT JUTT RESIDEA Autom Autom	JT N/T SSM/P
	移动应用		

通过以上步骤,完成了单点登录到Salesforce的功能。

# 2.标准协议模板使用指南

# 2.1. JWT 模板使用指南

# 一、概述

IDaaS平台提供了基于JWT标准协议实现的应用插件,使用该插件,业务系统可以快速的接入IDaaS平台,从 而完成单点登录。并且JWT应用插件支持从SP(业务系统)发起单点登录请求,跳转到IDaaS平台,进行登录, 再跳转回业务系统完成JWT令牌认证和业务系统的登录。同时,也支持从IDaaS平台直接发起单点登录请 求,传递JWT令牌后,在业务系统进行验证,完成登录。

本文档主要为JWT应用配置人员或开发人员提供完整的JWT应用配置过程或开发流程,并提供相应的SDK下载。

## 1.1 IDP/SP 发起单点登录的区别

Json web token (JWT),是一种用于双方之间传递安全信息的简洁的表述性声明规范。JWT作为一个开放的标准(RFC 7519),定义了一种简洁的方法用于通信双方之间以 Json 对象的形式安全的传递信息,该 token被设计为紧凑且安全的,特别适用于分布式站点的单点登录(SSO)场景。

同样, IDaaS平台提供的JWT单点登录应用插件支持IDP发起和SP发起, 二者主要共同点在于整个JWT的认证 流程(后半截)是相同的, 都需要业务系统开发JWT令牌验证和解析的接口, 并且需要根据解析出来的用户 子账户信息, 判断用户是否为该业务系统用户。如果需要跳转到特定页面, 用户可以通过在IDaaS平台填写 target\_url(填写地方请参考操作步骤 Step1 创建JWT应用), 或者在SP发起地址后面拼接target\_url请求参 数(注: 个别SP开发的针对线上老版本IDaaS的SSO, target\_url参数当初是以redirect\_url参数来接收 的), 以实现页面二次跳转, 达到deep-linking的目的, 上述功能和SAML中的RelayState是一致的。

IDP发起和SP发起二者的不同点在于从IDaaS平台发起单点登录,用户可以通过点击IDaaS平台首页的JWT应用,就能完成JWT令牌认证和业务系统的登录。从SP(业务系统)发起单点登录,系统不一定已经完成了 IDaaS平台的登录,或者登录信息过期失效,这时候IDaaS系统会跳转到登录页面,登录完成后,再继续完成 JWT令牌认证和业务系统的登录。



# 二、实现原理

上述时序图阐述了基于JWT发起SSO登录请求时的基本流程,该流程主要分为以下6个步骤:

1) 用户通过浏览器访问 IDaaS应用服务。

2) 浏览器向IDaaS发起单点登录请求。

3) IDaaS 生成 JWT token 令牌发送到业务系统。

4) 业务系统获取到 token 令牌,用提供的插件或方法解析验证 JWT token 令牌,解析成功获取到用户信息 并验证用户是否存在于业务系统中。

5) 业务应用服务器创建自己系统的请求会话, 然后跳转到指定路径。

6) 浏览器显示应用页面,完成sso登录。

验证通过: 业务系统重定向到用户首页, 或指定的二级页面。

验证失败: 业务系统拒绝登录并页面提示错误信息。

### 三、对接流程图

下面是开发对接一个新的应用支持JWT协议SSO的过程。



### 3.1 主要流程

该流程主要帮助开发者理解和集成一个SP应用支持JWT单点登录,从而完成整个JWT应用模版的使用。流程 主要分为以下6步:

### Step1 创建JWT应用

该步骤主要帮助开发者在IDaaS平台创建一个JWT应用,让SP(业务系统)系统能接入IDaaS平台的JWT SSO 登录,在该步骤中,主要是一些必要字段的填写,以便于完成后面的整个流程。

#### Step2 SDK下载

该步骤主要帮助开发者更加便捷的开发JWT token验证接口。使用IDaaS提供的JWT 验签SDK包,便于开发后续的JWT 验签接口。

#### Step3 业务系统研发

该步骤主要帮助开发者开发自己业务系统的JWT 验签接口,完成业务系统的用户验证和登录。

#### Step4 IDaaS上更新SSO地址

该步骤主要帮助开发者在完成JWT验签接口开发工作后,进行必要的接口验证工作。如果第一次在IDaaS平台 创建JWT应用时,填写的JWT 验签接口不准确(redirect\_uri),可以再次更新该地址。

#### Step5 单点登录效果验证

该步骤主要帮助开发者验证JWT应用配置的完整性和自己开发的JWT验签接口是否正确,验证SSO登录流程是 否能正确完成。

Step6 完成

### 四、操作步骤

4.1 Step1 创建JWT应用

# 4.1.1 登录 IDaaS 管理员平台。

使用 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

# 4.1.2 添加 JWT 应用。

在【应用】-【添加应用】中,找到应用名称为: JWT,点击右边【添加应用】按钮。(注意:请不要选择 成jwt证书)

28	后期协议	空制模板				
9	源加应用 本页面包: 应用9为1	3 含了所有已变体的可原加 同种:一种属支持后来的	应用利表、管理员可以选择需要 JWT、CAS、SAML管理包约5	使用的应用进行初始代 <b>数</b> 遭 2日,在应重可以通过承加的	. НТВОРИТ. 2019.6.0008-0.00-0-0.00-0.00-0.00-0.00-0.00-	
1945.	人应用名称				a	
应用	1944	应用名称	应用の	标签	NA.	应用类型
Ę	₹	CISTER	plugin_cs_oldc	CB, PC, OIDC	5個性学が進点ののための内部を書きな実施者、活用手可以提供給給ののためにきたがため、	PC窗户通
	٩.	CIS程序(別語器)	plugin_cs_multibrowser	CS, PC, Multi Browser	网络属国王的信制打开国王系统,并兼过铜彩路价行为地方式信任行或批批,进行于石砾形成正的信器的区径最大结构的2000年01开始应用	PC喜户跳
9	2	CAS(tEm)	plagin_cas_apereo	\$\$0, CAS	CAS(Central-Automotication Services、集合实际设备等。版本 2-00 是一种展开资格,应用的行用集中存在生的公,在集成基本和标准器的成合和存储器和存在实际了广泛在企业中的用,和集成集团,扩展性能的优化,	Web信用. 移动应用
DE	мо	Demo Plugin	plugin_demo	\$\$0	This is a Demo Plugin description( please change me)	Web信用
,	ļ	JWL	plugin_jwt	SSO, JWT	ハイド (JSON Yea Taken) 多辺原泉江戸川東市県の一冊番子 JSON 的計算信息、Gaud 使用 INT 旅行分析が広め合き発き(ISSO) 、ハイ 単合発達着手な対応定き、合しaud 共同小校会の広都使用も形式され、他連絡応用さ、他連絡応用されたの、使連絡応用されたの、使連絡応用されたの、使連絡応用されたの、使連絡応用されたの、使連絡応用されたの、使連絡応用されたの、使連絡に用されたの、使用	Web這用. 移动应用. PC有
Ĩ.	2	OAU/h2	plugin_oauth2	OAath2	ONIN 是一个月就到她想到你说心,应用可以通过 ONIN 获取到分離 access_biam,并我带令她来摇的挑嘴走得一些道,应用可以进用 ONIN 应用地放水车运动一身合想想。	Web应用
<u>p</u> e	мо	OA应用	plugin_oa001	550	This is a Densy Plugin decorption (plasse change me)	Web店用
5	5	SAML	plugin_saml	SSO, SAML	SMAL (Should Accedent Markya Language, 史全新編号近義編, 新年 24) 畫子 XMAL协议。 使用性性的 化分子分钟器 包括双方 (Chaud) 和品級方 (江市) 之间物造量价值售,实施量于阿希斯物力都作量低,SMAL 物心造成器的以近的论。 包括为外 的公司主任的基本中有可能"注意总规	Web应用
-	-	SAP GUI	plugin_sap_gui	\$\$0, C/\$	SAF GALEMARFINETSPERMENTERGENERGERENTERGENERGENERGENERGENERGE	РСВЛЯ
		Salosforce	stanin calectorre	880	Salactory ERTHRUBA-TEREN/SET ON THE (Dictions Relationship Management, ERTERRIG), OTOORG/TEREN/SET FARME END/SET, Dask THER SALA (NOR-THER) SALA (NOR	Webstell

# 4.1.3 填写信息并保存

根据需要填写如下信息:

修改应用 (JW	т) ×
♀ JWT应用使用	长度为2048的RS256加密算法。
图标	「
应用ID	idaas-cn-beijing-nc0pfjbm9nlplugin_jwt
* 应用名称	JWT
* 应用类型	✓ Web应用 ○ 移动应用 ○ PC客户端 "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,如果想在多个环境中都显示应用则勾选多个。
* redirect_uri	https://www.baidu.com 业务系统中的 JWT 单点容录地址,单点容录时 IDaaS 会携带 id token 带定向至该地址,应用系统校验 id token 获取用户身份以完成容录。支持输入多备地址,地址
	一一。 之间以请以换行分隔,在业务系统(SP)发起单点登录时,SP可以携带 redirect_uri 参数以指定单点登录地址,指定的地址必须完全匹配列表中的一条地址,否则 IDaaS 会拒绝跳转,在 IDaaS 发起单点登录,或者SP发起单点登录是未携带 redirect_uri 时,将默认选择该列表中的第一条地址。
target_url	https://www.qq.com/
	单点登录成功后,会在 IDaaS 跳转到 redirect_uri 时和id_token同时携带,一般用于跳转到deeplinking的二级菜单、指定页面等,此项可选。
SSO Binding	REDIRECT Y
ID_Token有效期	年末登城時水分式,REDIREDIAGELLANG 600 ID_Token的有效期,単位为: 秒
是否显示应用	授权給用户后,是否在用户首页显示。
*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)
	<ul> <li>账户映射(系统自动将主账户各称或指定的字段映射为应用的子账户)</li> <li>提交</li> <li>取消</li> </ul>

### IDaaS平台提供的参数, 具体如下:

- 1. 图标:业务应用的 logo 图片。
- 2. 应用 ID: IDaaS自动生成的应用 ID,不允许修改,且唯一。
- 3. 应用名称: 填写创建应用的名称。
- 4. 应用类型: 代表该服务支持的设备类型,标记使用。
- 5.SSO Binding: 单点登录请求方式, REDIRECT 为 GET 类型, 也可选择 POST。

7.ID\_Token有效期:单位秒。

8.是否显示应用:授权给用户后,是否在用户的IDaaS平台首页显示,默认开启。若关闭,用户登录IDaaS平台首页,将看不到该应用。

9.账户关联方式:

a.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)

b.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)

SP(业务系统)需要考虑的参数:

一个全新的应用从不支持JWT,到支持,需要开发几个URL,以下为两个重要参数:

1. redirect\_uri: 业务系统中(或 PC 程序)的 JWT SSO 地址,在单点登录时 IDaaS 将向该地址用[GET]方式发送 ID\_Token 信息,参数名为id\_Token,业务系统通过 ID\_Token 与 Public Key 可获取JWT token中的用户信息。

2. target\_url: 业务系统中在通过JWT系统完成身份认证成功后,重定向的 URI。一般是一个http开头的URI, 用于跳转到二级页面等。若设置了该 URI,在IDaaS平台在完成JWT协议身份认证成功时,会以参数 target\_url传递该值,若未设置该值,若此时SP发起的SSO请求中有参数target\_url,则会按照请求参数传递 该值,此项可选。如果target\_url为空,由SP决定跳转到哪个页面,一般是默认的门户页面。

### 4.1.4 导出公钥

基于JWT的非对称签名/验签机制,完成上面应用创建,私钥保存在IDaaS 后台,作为签名使用,公钥需要 导出传递给SP验签使用。在【应用列表】中,就可以找到新创建的应用。点击【详情】按钮,点击【查看 详情】。



### 找到 JWT PublicKey

复制粘贴到文本txt,或者使用下方导出,都可以将 JWT PublicKey 导出。将其交给需要接入JWT协议认证的 SP业务系统,用作 ID\_Token 的验签解析。

应用详情(JWT 测	式)
应用ID	lin0219plugin_jwt3
应用名称	JWT 测试
redirect_uri	https://www.aliyun.com/product/idaas
Target_link_uri	无
JWT Keyld	4897472017407736362
JWT PublicKey	{"kty":"RSA","kid":"4897472017407736362","alg":"RS256","n":"2sOSejw9ETttQ14AqBQ1mnCKrHZEnWWn1 H3W3zQO_b1rK6oWCfl-7_fVSeR2CiOS2boaTnCMialeChVXTL6A86fL1Eunnl_zpoldVibytfaGJu10gKLCzgf qMg8eHAV5RUk2UjpwPWAbgSzmAqnRitFHuxgIrjwg1Mzi07Q323INiL0wZLmIsvtQgds7FNyUCQgXMgx1W SyfbDX9YTt9ta8bVj-96ExhDuumOHhGtL5sXkw0H-qVwRUvUDIMVJF5KjkV33dT32hNnzR7_DB_OpMbqHB _ICdeokr7LcZC7iJ89Ru9LEUX2gWU3Pj8gaCa1bA0VFIW7_mA9CdNH5GqFQ","e":"AQAB"}
	导出PKCS8公钥 导出PKCS1公钥
SSO Binding	REDIRECT
ID_Token有效期	600秒
账户关联方式	账户关联

# 4.2 Step2 SDK下载

在这里,IDP配置好了, 第三方业务系统SP就要开始研发的准备工作了。所有需要接入JWT应用源的SP都需要开发相对应的JWT id\_token的SSO接收接口, 该接口主要用于id\_token的解析, 签名验证, 和用户信息的抽取。然后在业务系统中对比获取到的用户信息, 对比成功后, 创建业务系统自己的登录会话, 完成SSO登录。

IDaaS提供 4 种语言的 SDK 集成方式: JAVA/PHP/.NET/Python:

JAVA SDK下载

JAVA SDK - JDK 1.6

JAVA SDK - JDK 1.7

JAVA SDK - JDK 1.8

PHP SDK下载

PHP-JWT-SDK

.NET SDK下载

.NET-JWT-SDK

Python SDK下载

### Python-JWT-SDK

当然,如果您的业务系统是除此之外其他语言也可以进行对接,需要您自行编写解析 ID\_T oken 的代码,需要可以参考

JWT 官网。

### 4.3 Step3 业务系统研发

如上所述, SP研发核心需要考虑的:

- 1) 能够接收到令牌
- 2) 能够成功验签解析令牌,拿到用户Sub信息
- 3) 匹配用户信息是否与当前自己的子账号一致,完成匹配之后,创建业务系统自己的会话

4) 跳转至用户首页

### 4.3.1 JAVA 插件式集成

### 配置环境

根据java JDK版本,选择相对应的SDK版本,如常用的java JDK版本为1.8,请选择

#### JAVA SDK - JDK 1.8.

#### 接收令牌

假设IDaaS通过POST或Redirect 将id\_token 传递到SP, SP首先需要提供一个SSO的URL

### 接收示例:

url 示例: https://localhost/JWT/sso/login?id\_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEwMjQxNjE0NzI2Nzg2MjI0NjgifQ

//id\_token 是 IDaaS 请求时带来的,在 requestParam 里获取,PublicKey是在 IDaaS 里注册应用时生成的,注册完 可见,此示例代码是获取用户信息。 // JWT SSO @RequestMapping(value = "/JWT/sso/login") public String SSO Url(@RequestParam String id\_token, String target\_url, Model model, HttpServletReques t request){ //1.接收方法为GET方式,参数名为 id\_token //2.<解析令牌>为解析 id\_token 并验证代码

}

### 解析令牌

拿到id\_token 后,为了保证不是重放或中间人攻击,需要对其进行验签,前面导出的PublicKey主要被用于这个目的。注意,不同语言的SDK可能用到的PublicKey格式是不同的。

```
//1.使用公钥,解析 id_token
//使用PublicKey解析上一步获取的 id_token 令牌,并验证id_token
DingdangUserRetriever retriever = new DingdangUserRetriever(id_token, PublicKey);
DingdangUserRetriever.User user = null;
try {
   //2.获取用户信息
   user = retriever.retrieve();} catch (Exception e) {
   LOG.warn( "Retrieve SSO user failed", e);
   return "error";
}
//3.判断用户名是否在自己系统存在,isExistedUsername()方法为业务系统自行判断数据库中是否存在
if (isExistedUsername(user.getUsername())) {
   //4.如果用户存在,则登录成功,然后创建业务系统自己的会话(如session的更新),具体操作,根据各自业务系
统的需要进行开发,以下只做示例
   User SPUser = userService.updateLoginTimes(user.getUsername());
   request.getSession ().setAttribute(HttpSessionSecurityContextRepository.SPRING_SECURITY_CONTEX
T_KEY, saveSecurity(SPUser));
   //5.如果请求参数中带有target_url(注:线上有些版本参数名为redirect_url),那么返回此指定的url页面
 if (StringUtils.isNotEmpty(target_url)) {
      return "redirect:" + target_url;
   }
   //6.否则返回SP自定义的默认操作页面
   return "redirect:../../index" ;
} else {
   //7.如果用户不存在,返回登录失败页面,提示用户不存在
   model.addAttribute( "error", "username { "+ user.getUsername() + "} not exist");
   return "error";
}
```

# 4.3.2 PHP插件式集成

### 配置环境

```
在本例中,使用composer管理一个第三方JWT库(可选)。
```

```
同样, 假设IDaaS通过POST或Redirect 将id_token 传递到SP, SP首先需要提供一个SSO的URL。
```

### 接收示例:

url 示例:

 $https://localhost/JWT/sso/login?id\_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEwMjQxNjE0NzI2Nzg2MjI0NjgifQ$ 

### 接收令牌

如上, JWT 的 id\_token 将会以url参数的方式传进callback页面(同JAVA的),直接将其读取出来:

```
/* 使用composer 载入 php-JWT第三方库
* 命令行 composer require firebase/php-JWT
* 库链接: https://github.com/firebase/php-JWT
*使用Firebase的这个第三方库来实现对JWT的解密,如果不用composer的话,请自行添加源文件
*你也可以使用其他能对 JWT token 进行RS256解码的工具或库
*/
// 在这里将 JWT 库引入,在这里为了便捷demo直接使用
// 推荐使用
require 'vendor/autoload.php';
use \Firebase\ JWT \ JWT ;
// 本地存储public key公钥的位置
$public_key_location = "LOCATION/TO/YOUR/PUBLIC-KEY/XXX.pem";
//读取公钥信息,公钥在这里存储在一个.pem文件内
$public_key = file_get_contents($public_key_location);
// 从url的参数中读取 id_token ,即令牌
if (!empty($_GET[ "id_token "])) {
   $JWT = $_GET[ "id_token "];
   // 这里继续第二步: 解析令牌
}
```

获取到id\_token之后, 接下来就是对令牌的解析和验签步骤。

解析令牌

拿到id\_token 后,为了保证不是重放或中间人攻击,需要对其进行验签,前面导出的PublicKey主要被用于这个目的。利用第三方库 php-JWT进行验签,获取到用户信息。验证通过后创建业务系统自己的会话,然后再跳转到SP登录后页面,失败则拒绝,返回SSO失败页面:

```
phptry{
   /**
   * You can add a leeway to account for when there is a clock skew times between
   * the signing and verifying servers. It is recommended that this leeway should
   * not be bigger than a few minutes.
   * Source: http://self-issued.info/docs/draft-ietf-oauth-json-web-token.html#nbfDef
   */
   // Firebase的 JWT 库的一个参数,不出问题的话可以忽略
   //(可选)当服务器时间与本地时间不符时,可以通过这个leeway参数来调整容错
   JWT::$leeway = 60; // $leeway in seconds
   //使用公钥、使用RS256算法对 JWT (即第一步传进来的 id_token )进行解密
   $decoded = JWT::decode($JWT, $public_key, array('RS256'));
   // 将解密的结果从class转化成PHP array
   $decoded_array = (array) $decoded;
   //打印出解密的结果,成功!
   print("解密结果:<br>");
   foreach ($decoded_array as $key => $value) {
      print $key . ": ".$value . "<br>";
   }
   // 获取到用户信息后,判断该用户是否存在于你的系统内
   if (userExistsInSystem()) {
      // 如果用户存在,那么登录成功
  //登录成功后,创建业务系统自己的会话,略
  //会话创建完成后,如果有target_url参数,跳转到该地址
   } else {
      // 如果用户不存在,那么登录失败,跳转到显示错误页面
   }
catch(Exception $e) {
 print "错误:".$e->getMessage();
```

# 4.3.3 .NET插件式集成

### 配置环境

}

.NET Framework 4及以上。

同样, 假设IDaaS通过POST或Redirect 将id\_token 传递到SP, SP首先需要提供一个SSO的URL。

接收示例:

## url示例:

https://localhost/JWT/sso/login?id\_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEwMjQxNjE0NzI2Nzg2MjI0NjgifQ

### 接收令牌

如上, JWT 的 id token 将会以url参数的方式传进callback页面(同JAVA的)

解析令牌

拿到id\_token 后,为了保证不是重放或中间人攻击,需要对其进行验签,前面导出的PublicKey主要被用于 这个目的。如果成功,获取用户信息,然后创建业务系统自己的会话,最后跳转进入SP用户登录后的页面, 否则返回SSO失败页面。

```
//1.使用公钥,解析 id_token
string username;
DingdangSDK.DingdangUserRetriever retriever = new DingdangSDK.DingdangUserRetriever(id_token, Pu
blicKey);
DingdangSDK.User user = null;
//2.获取用户信息
user = retriever.retrieve();
username = user.sub;
//3.判断用户名是否在自己系统存在
//4.如果用户存在,则登录成功,创建业务系统自己的会话,返回登录成功后的页面,略
//5.如果参数中有target_url,那么返回此SP指定的url页面
//6.否则返回系统默认操作页面
//7.如果用户不存在,返回登录失败页面,提示用户不存在
```

# 4.3.4 python插件式集成

下载资源库

```
本Python JWT 示例使用Py JWT 库来进行 JWT 的解析。
```

假设IDaaS通过POST或Redirect 将id\_token 传递到SP, SP首先需要提供一个SSO的URL。

接收示例:

```
url示例:
https://172.168.0.1/JWT/sso/login?id_token=eyJhbGciOiJSUzI1NiIsImtpZCI6IjEwMjQxNjE0NzI2Nzg2MjI0Njgif
Q
```

```
// 库的 github 链接 https://github.com/jpadilla/pyJWT
pip install Py JWT
// 注: CentOS系统如果使用时无法导入算法 RSAAlgorthm时需要下载pyJWT的2个依赖包
yum install ibffi-devel
pip install cryptography
```

### 接收令牌

如上, JWT 的 id\_token 将会以url参数的方式传进callback页面(同JAVA的)。

def get\_id token ( token ): if not token .strip(): print(' token 信息不能为空') else: //这里继续第二步:解析令牌 get\_id token (my\_id token ); // 运行程序

### 解析令牌

拿到id\_token 后,为了保证不是重放或中间人攻击,需要对其进行验签,获取用户信息,前面导出的 PublicKey主要被用于这个目的。验证通过后创建业务系统自己的会话,然后再跳转到SP登录后页面,失败 则拒绝,返回SSO失败页面。注意,Python库需要的PublicKey格式不一定是和其它一致的。开发前需要在 IT管理员权限下前往应用->详细->导出 PKCS8 公钥来获取解密 JWT 用的公钥,并安全地放置在能访问到的目 录内。

## 2.解析令牌 通过JWT解密库,使用公钥对传入的 id\_token 进行解密。将公钥以字符串的形式从文件中读取出来,并作为key进行 解密: // 引入用到的包文件 import JWT import json from JWT.algorithms import RSAAlgorithm from JWT.utils import force\_bytes from utils import key\_path //本例中key\_path辅助方法是写在utils工具类中的 def get\_user\_ifon( id\_token ): try: algo = RSAAlgorithm(RSAAlgorithm.SHA256) pem\_key = open(key\_path('D:\pythonDemo\key\public\_key\_pkc8.pem'), 'r') public\_key = algo.prepare\_key(pem\_key.read()) token\_info = JWT.decode(force\_bytes( id\_token ),key=public\_key,verify=True) user\_info = json.loads(json.dumps( token\_info)) username = user\_info['sub'] print(username) #3.判断用户名是否在自己系统存在 #4.如果用户存在,则登录成功,创建业务系统自己的会话,返回登录成功后的页面,略 #5.如果参数中有target\_url,那么返回此指定url页面 #6.否则返回系统默认操作页面 #7. 如果用户不存在, 返回登录失败页面, 提示用户不存在 except Exception as e: print(e)

上面用到的key\_path方法是用来获取存放在硬盘上的public key位置的辅助方法,具体如下:

def key\_path (key\_name):
 return os.path.join(os.path.dirname(os.path.realpath(\_\_file\_\_)), 'keys', key\_name)

总之,在完成JWT令牌的接收,验签和解析之后,业务系统需要根据JWT令牌解析出来的用户信息,判断用 户是否存在于当前业务系统中。如果用户存在,业务系统创建自己系统的会话请求(如存放session,生成 cookie等,请根据业务系统各自要求去实现),以保证用户的登录状态。然后判断是否有target\_url参数, 如果有该参数,那么返回该参数指定的url页面,从而完成SSO的登录。

# 4.4 Step4 IDaaS上更新SSO地址

由于在第一步创建应用时,SSO单点登录地址(即redirect\_uri)不一定是SP开发完成后正确的URL。所以, 当业务系统开发工作结束后,有可能需要再返回 IDaaS 平台,以IT管理员身份,将这个地址进行更新,后续 才能进行下一步的联调测试工作。

WINDERBERKERADAVARRINGSOSSINERE.           WINDERBERKERADAVARRINGSOSSINERE.           WINDERBERKERADAVARRINGSOSSINERE.           WINDERBERKERADAVARRINGSOSSINERE.           WINDERBERKERADAVARRINGSOSSINERE.           BIR           WINDERBERKERADAVARRINGSOSSINERE.           BIRD           BIRD           BIRD           MINDERBERKERADAVARRING           ADDA           BIRD           BIRD           BIRD           BIRD           BIRD           BIRD           BIRD           BIRD           BIRDARDER           BIRDARDERS	
● WT直用使用长度为2044的FR525000編集法。         ■标         ■标         ● 上板文件         ■大小不過はWE         ● 上板文件         ● 上板文件         ■市         ● 上板文件         ● 広用の         Im0219pugin_LM3         ● 広用名称         ● Venden ● Strade ● Care/M         • Venden ● Strade ● Strade ● Care/M         • Vende ● Strade ● Strade ●	
BR     IDEN       BL     L H호QL       BL     L H호QL       BL     L H호QL       BL     L H호QL       BL     BL       D     Int0210plugin_uM3       IntD     Int0210plugin_uM3       IntD     INT BIK       IntD     INT BIK       IntD     INT BIK       IntDL	
应用D     Inn219plugin_wt3       ・应用名称     JV/T 题式       ・应用名称     『Wob应用 ③ 移动应用 ④ PC客户读 "Wob应用 ④ 移动应用 ④ PC客户读 "Wob应用和PC客户读了会在用户Wob使用环境中显示、移动应用只会在用户客户读中显示如果想在多个环境中都显示应用则构造多个。       ・redirect_uri     Ihtps://www.ailyun.com/product/idaas 业务系统中(或 PC 程序)的 JWT SSO 地址、在单点型最对 IDaaS 将向读地址用(GET)方式发送 ID_Token 信息、参数合为ID_Token、业务系统通过 ID_Token 号 Public Key 可译 和业务系统中的用户信息、 如果在业务系统(SP)发起稳定、请求 SP 登录地址封如果携带 Service 参数 IDaaS 经检验合法性、成功后会将测试器重定向到运地址,并携带ID_Token身份会模。       Target_link_uri     单点包表示的数块地址、知: http://www.com/service/message 业务系统中在 WT SSO 成功后重定向的 URI, 一般用于预除到二级集单等,者设置了该 URI, 在 JWT SSO 时会认参数 Target_link_uri 优先传递说语、截并设置读值、此时者SSO中有请求参数 Target_link_uri 」、则会按照请求参数供通读值、此项词选。       是否包含用户角色     D_Token中最否包含用户角色信息。	
・ 应用系称     ・ 应用系称     ・ 应用系和     ・ 定面     ・ 正面     ・	
<ul> <li>・ 应用共型         <ul> <li>● Web应用</li></ul></li></ul>	
・ redirect_uri https://www.aliyun.com/product/idaas 业务系统中(或 PC 程序)的 JWT SSO 地址,在单点型最对 IDaaS 将向该地址用(GET)方式发送 ID_Token 信息,参数名为ID_Token,业务系统通过 ID_Token 与 Public Key 可E 取业务系统中的用户信息,如果在业务系统(SP)发起登录、请求 SP 登录地址时如果携带 Service 参数 IDaaS 会检验会法性,成功后会将测范器重定向到该地址,并携带ID_Token身份令裸。 Target_link_uri 单点管表后的翻转地址,如: http://www.cox.com/service/message 业务系统中在 JWT SSO 成功后重定向的 URI,一般用于跳转到二级常单等,若设置了该 URI,在 JWT SSO 时会以参数 Target_link_uri 优先传递读值,此时若SSO中有请求参数 Target_link_uri 是否包含用户角色 ID_Token中显否包含用户角色信息。	
Target_link_uri     单点受受后的期转地址,如: http://www.cox.com/service/message       业务系统中在 JWT SSO 成功后重定向的 URI,一般用于跳转到二级集单等,若设置了该 URI,在 JWT SSO 时会以参数 Target_link_uri 优先传递谅值,此时若SSO中有请求参数 Target_link_i,则会按照请求参数传递读值,此项可选。       星否包含用户角色     ID_Token中显否包含用户角色信息。	
显否包含用户角色 ID_Token中显否包含用户角色信息。	ur
SSO Binding REDIRECT ~ 单点登陆请求方式,REDIRECT为GET英型	
ID_Token有效期 600 ID_Token的有效期,单位为: 秒	
基否显示应用 授权途用户后,是否在用户首页显示。	
● 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,用户该加后需要管理员审批)	
○ 取户"缺省) (系統局和時主地户名标和局面的子服務部方加用的子地户)           提交         取消	

# 4.5 Step5 单点登录效果验证

# 4.5.1 从IDaaS发起单点登录

在完成IDaaS平台的redirect\_uri更新之后,开发者可以新建一个测试账号进行单点登录效果验证,以确保JWT 的应用源接入成功。

# 4.5.1.1 新建一个普通账号

统一身份认证	平台			消息 10. 数认管理员 • 切脱语言 •
概览		机构及组		数据字典
快速入门 应用 应用列表	^	机构及组 留理员在当前页面对组织架构、部门及其包含的 在左侧的组织架构称中,可以右键。而击革个部门	组、账户进行管理。也可以使用 AD、LDAP 呃 Exoet文件统力式配置导入或同步。 13时其进行操作,也可以左键选择某个部门,并在右侧为共进行创建集合。创建组、创建部门等操作。	×
添加应用 月户目录 机构及4月	^	组织架构	PS探閱系统 查看评情	岗位变动 >   导入 >   导出 >   配置 LDAP   配置 钉钉同步
账户管理 公举管理		在这里对组织织构进行管理。左键可选择 × 组织机构,右键可对组织机构进行管理。	账户 组 组织机构	
证	^			
RADIUS 证书管理		世」 ○ ■ #12     日 ○ ② #13     ① ● 新13     ③ ● 新13     ③ ● ○ ● 新13     ③	續号 账户名称 显示名称 类型 目录	操作
2	^		- 1 自建账户 /	修改转动 账户同步 同步记录 高职
权限系统 应用授权				修改 转向 账户同步 同步记录 离职
计 它管理 ●	ž			1781以 34800 340 <sup>-11</sup> 99岁 19岁纪录 黑歌 修改 转岗 账户同步 同步记录 高职
置	~		5 自建账户 /	修改转资 账户同步 同步记录 高职

# 4.5.1.2 账号授权

在新建账号时,会自动授权,比如可以看到给授权的应用,然后点击下一步,完成账号授权。

增量同步		×
✓ LDAP同步 将数据同步至所有LDAP	2 应用授权 将自动继承父级的应用授权	<ul> <li>3 SCIM同步</li> <li>通过SCIM将数据同步至已授权</li> <li>应用</li> </ul>
将自动继承父级的应用权限,身	具体如下:	NACT
JWT Sabel-defilo	Л	共2条 〈 1 〉
		下一步取消

或者用另外一个方式,使用【授权】-【应用授权】-【按账户授权应用】功能,给账号分配需要测试的JWT 应用。

统一身份认证平台			消息 🕕 数认管理员 🖌 切换语言 🗸
概览	应用授权		
快速入门	按应用授权组织机构/组 按组织机构/组授权应用	按账户授权应用 按应用授权账户 按分类授权应用	
应用 ^ 应用列表 添加应用 用户目录 ^ 机构及组	技能/小授权应用  直接方版注意/小授权版定度用。  提示:这里展示的并不是 除号是否有某应用权用 可以通过第户管理最看到某个很产所拥有的全部品	1」,而是「账号是否直接授权到某应用」。账号同样可以通过转所重组织机构,所重组等来进获利用权限信息。	× 观应用的印刷。
账户管理 分类管理	账户(2)	<b>应用数 (13)</b> 已授权(1)个	
认证 ^	saber	请输入应用名称进行搜索	٩
认证源 RADIUS	saber001 >	应用名称	应用ID
证书管理	saber >	対態 TWL 💟	lin0219plugin_jwt3
授权 个	共2条 〈 1 〉	TWL	lin0219plugin_jwt1
应用授权		OAuth2	lin0219plugin_oauth2
审计 、		saber-demo	lin0219plugin_jwt
其它管理 ~		調訊企业邮	lin0219plugin_exmail2
(注直 ) ~		则试应用1	lin0219jwt7

# 4.5.1.3 使用测试账号登录

使用测试账号登录后,即可看到创建的JWT测试应用 logo图标。

统一认证身份平台	消息 🕕	۵	切换语言 🗸
欢迎·IDaaS	我的应用		
主导航 ^	Web应用		
首页			
应用管理			
应用子账户			
设置 ^	JW1		
我的账户	bill the second se		
二次认证			
我的消息			
我的日志			
	移动应用		
	当前没有授权的移动应用。		

### 注: 若此时无法看到图标, 请检查

- (1) 应用是否开启?(【应用列表】查看及开启)
- (2)账号是否被授予应用权限?(【应用授权】查看及授权)

### 4.5.1.4 业务系统检查是否能获取到 id\_Token

下一步, 点击这个图标后, 会触发一个SSO URL, 通过检查IDaaS系统发送的id\_token 和业务系统(SP) 收到的id\_token是否一致, 从而确保业务系统能正确获取id\_token。

### SSO URL 示例:

https://www.example.com/sso/login?id\_token=xxxx

- (1) 首先登录IDaaS系统
- (2) 点击应用 logo
- (3) 可以在浏览器地址栏中看到 id\_token 及SP二级页面的target\_url信息,例如:

👔 aliyun.com/product/idaas?id\_token=eyJhbGciOiJSUzI1NilsImtpZCI6ljQ4OTc0NzlwMTc0MDc3MzYzNjlifQ.eyJlbWFpbCI6lnFxcUBxcS5jb20iLCJuYW1IIjoi5bCP5pa5liwibW9iaWxIIjpud... )就知道 📒 IDP 📃 学习 📒 其他 📒 IDP4 M 阿里邮箱 🔥 云笔记 🍥 NATAPP - 🌠 周报 🚺 aone 🍠 云知-数字化产品管... 扂 飞天文档数据看板 🌙 我的知识库·语雀 臼 应用身份服务-帮助 (4) 也可以使用浏览器的 [开发者工具] 看到 id\_token 信息,



(5)如果id\_token 正常,此时业务系统就需要检查是否能够收到 IDaaS 发送的 id\_token 并且成功解析验 签,获取用户信息。

# 4.5.1.5 检查是否能正确跳转到业务系统指定页面

如业务系统成功获取并解析 id\_token 正常,就应该能成功创建业务系统自己的会话(如session更新,生成 cookie等),然后跳转到业务系统指定的页面。

# 4.5.2 从业务系统(SP)发起单点登录

上面介绍完了IDP发起,下面介绍SP发起的SSO过程。

SP发起的URL地址由IDaaS平台在创建JWT应用时,自动创建,用户无法修改。

### URL示例:

https://<idaas>/enduser/sp/sso/{应用ID}?enterpriseId={公司ID} 业务系统(SP)需要把SSO单点登录请求发送到该地址。 从SP发起的SSO单点登录请求,一般情况下,都是用户在业务系统的页面首先进行操作,如用户点击邮箱地 址(htttps://www.example.com/?email=xxxx),此时,用户在未登录的情况下,邮箱服务需要把用户页面 重定向到SP发起地址。然后用户在IDaaS完成登录,最后再次跳转到登录前的业务系统页面,即用户邮箱地 址(htttps://www.example.com/?email=xxxx)。

### 4.5.2.1 业务系统配置SP发起地址

一般情况下, SP的开发者需要开发相应的代码来完成整个SP发起的 SSO流程。

首先,开发者需要在业务系统开发中,添加SP发起地址(如业务系统首页的第三方登录按钮,或者在业务系统的登录拦截器),当用户需要登录业务系统时,页面需要重定向到SP发起地址,同时SP系统应该把当前的URL,生成一个随机数关联保存在本地,把这个随机数作为target\_url传递给IDaaS。

SP发起地址获取方式:

请在IT管理员权限下前往应用->应用信息->点击【SP发起地址】进行复制。

统一身份认证平	诒				消息 📀 🛛 默认管理员 🗸 切换语言 🗸
概览 快速入门		加工H7938 管理员可以在当前页面管理已经添加的所有应用,当添加完应用后,应该确认应用处于后用状态,非	应用可以实现单点 <b>登录和数据同</b> 步能力。 针已经完成了授权。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	168.
应用 应用列表	^	送加於用 時後入並用名称 应用图标 应用名称	Q 应用D 应用分类	应用状态	二次从正状态 摄作
洞山並用 用户目录 机构及组	^	TWL	cfplugin_jwt		◎ ※ 授权 详情 ▲
账户管理 分类管理		应用信息	认证信息	账户信息 - 同步	账户信息 - 子账户
认证 认证原 RADIUS	^	应用的详细信息 重 <b>看详情</b> 修改应用 删除应用	应用的邮点登录地址 IDaaS发起地址 SP发起地址	SCIM协议设置以及把组织机构、组同步推送至应用 同步机构 SCIM配置	平台主账户与逾用系统中子账户的关款表 查看如用子账户
业书官理 授权 权限系统	^	授权信息 应用与人员组织的授权关系	<b>审计信息</b> 查看应用系统详细的操作日志	API 是否对应用开放系统API	<b>管理应用内权限</b> 管理应用内菜单与功能积限
应用授权 审计	×	授权	查看日志 查看同步记录	API Key API Secret	横定权限系统
其它管理	~	CAS * CAS1 test2	cfplugin_cas12		● 授权 详情 ▼

#### SP发起地址示例:

https://<idaas>/enduser/sp/sso/{应用ID}?enterpriseId={公司ID}&target\_url=XXX

其中:

target\_url: 该参数为SP系统开发者可选参数,如果添加了该参数,IDaaS在完成登录后,会优先使用该值, 覆盖在创建JWT应用时,填写的target\_url,并把该值返回给SP。

应用ID:在IT管理员权限下前往应用列表 -> JWT应用源的应用ID。

统一身份认证平	诒						消息 🕗	默认管理员 ~	切换语言 ~
概览		应用列表							应用分类
快連入门									×
应用 <b>应用列表</b> 添加应用	^	应用列見 「 管理员可 当添加引	复 可以在当前页面管理已经添加 15应用后,应该确认应用处于。	的所有应用,应用可以实现 <b>单点登录和数据同</b> 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。		
用户目录	^	添加应用	約入应用名称		Q				
形//inj/x组 账户管理		应用图标	应用名称	应用ID	应用分类	应用状态	二次认证状态	操作	
分类管理		J	JWT	cfplugin_jwt			×	授权详情,	
认证源	^	CAS *	CAS1 test2	cfplugin_cas12				授权详情。	
RADIUS 证书管理		CAS *	CAS1 Plugin	cfplugin_cas11				授权详情,	•
授权 权限系统	^	CAS *	CAS1 test	cfplugin_cas1				授权 详情	
应用授权 审计	~	C	CAS(标准)	cfplugin_cas_apereo				授权详情。	
其它管理 <sup>●</sup> 设置	* *					共5	& <	10 条/页 > 跳至	1 页

### 公司ID:在IT管理员权限下前往设置 -> 个性化设置 -> 公司信息 查看。

统一身份认证	平台			消息 🕗	默认管理员 ~	切换语言 ~	
快速入门							
应用	^		◎ 上传文件				
应用列表 添加应用			图片大小不過过1486,宽高比量好是1.1,不能大于2.1或小于1.2 在用户登录员会显示公司图标				
用户目录	^	*公司全称	赏试租户				
机构及组	- 1		公司全称, 如:北京 XXX 技术有限公司				
账户管理	- 1	*公司简称	测试阻户				
分类管理		_	公司節称				
认证	^	*公司ID	d and a second se				
以证课	- 1		公司 ID 具有唯一性,只能包括字母与数字,不能有汉字,且不允许变更				
征书管理	- 1	* 部箱					
1647			公司邮箱是公司管理员登录 IDaaS 平台的账户,唯一;如若想改请到用户的"我的账户"中修改				
权限系统		电话	电话				
应用授权	- 1		公司电话号码,如1010-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx				
审计	~	公司网址	公司网址				
其它管理	v		公司网班上,知:http://www.xbobox.com				
设置	^	公司地址	公司地址				
个性化设置		公司介绍					
安全设置				11			

# 4.5.2.2 从业务系统(SP)发起登录

在浏览器输入业务系统(SP)的地址,比如用户现在需要登录邮箱,此时用户首先点击的就是邮箱地址(如 htttps://www.example.com/?email=xxxx),然后邮箱服务需要把浏览器重定向到业务系统配置好的SP发起地址。

### SP发起地址示例:

https://<idaas>/enduser/sp/sso/{应用ID}?enterpriseId={公司ID}&target\_url=XXX

如果用户未登录,会跳转到IDaaS统一登录页面,进行登录。登录完成后,IDaaS系统会将浏览器重定向到 redirect\_uri地址(redirect\_uri地址请在IDaaS平台 ->应用列表->应用信息里面查看)。
应用详情 (J	WT)
图标	JWT
应用ID	idaas-cn-beijing-nc0pfjbm9nlplugin_jwt
应用名称	TWL
应用Uuid	
redirect_uri	https://www.baidu.com
target_url	https://www.qq.com/
JWT Keyld	5756931801513916833
JWT PublicKey	{"kty":"RSA","kid":"5756931801513916833","alg":"RS256","n":"IK-riTxG3Ex7nM3MqS404qAq31DilHingDaQmPhHD_fm4BabMf- Dfdr/YEUBPrOA9NKgNwR3oMhb15ypgk9TyhVlkmMAY8F49Wrbq7ZFdj_oo6PxJrlL8SyZUkRqtJR0w254gfjEfikvj0d7OMsAE4mDb8ejLjXXpppgDDj5EvKC07T6AqeL nwkjQjJxUFQ4EPFFPPi-CN04jmyO1XsXb-ArUH1v4yYCN96VjIX8SPTZYSUb_h9KGTi58qTLxtxpnqWqo7jgdsWwMApD-jk81I0BzeGnidPSq-sKOObikZ9u-U6ao1zrS- O0kwwLZkelk9ljkh9J2V1tGUU6oNSu8w","e":"AQAB"}
	导出PKCS8公钥 导出PKCS1公钥
SSO Binding	REDIRECT
ID_Token有效期	600Eb
签发者ID	https://ecisyscglx.login.aliyunidaas.com/ 会出现在ID_Token的"iss"字段中
接收者ID	idaas-cn-beijing-nc0pfjbm9nlplugin_jwt 会出现在ID_Token的"aud"字段中
账户关联方式	账户关联
应用状态	禁用

并且带上id\_token及target\_url参数。为了兼容老版本IDaaS平台,早期使用redirect\_url来起到target\_url相同的效果的,注意redirect\_url和 redirect\_uri的区别,所以现在请求参数中会返回target\_url和redirect\_url两个相同值的参数,参数的值都为需要跳转的二级页面地址,并且优先使用业务系统在SP发起地址里拼接的target\_url。当业务系统没有在SP发起地址里拼接具体的target\_url参数时,IDaaS系统会采用在创建JWT应用时,填写默认的target\_url。

#### redirect\_uri地址示例:

https://www.example.com/sso/login?id\_token=xxxx&redirect\_url=yyyy&target\_url=yyyy

如下图所示, 会有3个参数拼接到地址后面。

☆ 百度一下, 你就知道 × +			- a ×						
← → Ů A https://www	.baidu.com/?id_token=eyJhbGciOiJSUzI1NiIsImtpZCI6Ij	U3NTY5MzE4MDE1MTM5MTY4MzMifQ.eyJlbWFpbCl6b	6bnVsbCwibmFtZSI6ImNmX3Rlc3QiLCJtb2JpbGUiOilxMzk4MDUyMjk1OCIsImV4dGVybmF 🗴 左 🖀 🔮 …						
★ HATP: USCUM A ← → ○ A https://www. 新用 hae123 均差 税元 5	tbaidu.com/?id_token=eyJhbGciOüSUz11NiisImtpZCI6j 地域 京木 夏多 日本が参 1 外交新回应構造中国際構成情形に 2 属虹頂開現取194±後の時刊	UJINTV5MzE4MDE1MTM5MTV4MzMifQ_eyJbWFpbCG6b 百度 ① 百成一下 () 第一時 4 女気人始張成館私10時版元亡 5 *を下おい子公司機能知識度	Jöbn/SbCwibm/Fi/2516/im/Nm/X3Rkl3QiLC/th22pbGU/DikiA/k44MDUy/MjKl1OCIsim/V4G/Vybm/F ☆     ☆     ★						
	<ul> <li>第625日年1月10日(1997)</li> <li>第625日年期天平坦松影响中国</li> </ul>	3 61747月17日之间的加利利用度 6 被波化学物质女主动合致音响后	<ul> <li>wenku02-01-bits</li> <li>jere Fetch User: 12</li> <li>jere Fetch User: 13</li> <li>jere Fetch User: 14</li> <li>User Agent: Net111a/3.0 (Listope III 10.0; Listope IIII 10.0; Listope III 10.0; Listope</li></ul>						

最后业务系统(SP)完成JWT令牌的验签和用户信息匹配的工作。验签成功后,业务系统将创建本系统的请求会话,然后把浏览器重定向到target\_url地址。

## 4.6 Step6 完成

当所有测试工作结束后,就在 IDaaS 上完成了 SSO 单点登录的对接工作。如果IDaaS系统和SP(业务系统)都是使用的测试环境,那么在正式上线切换时,需要再次将 JWT 模板中的地址修改为正式生产环境的地址。

## 五、FAQ

## 5.1 提示MAVEN库错误

如果是找不到这个maven库依赖:



该SDK是由IDaaS提供不是从官方下载,没有官方的maven仓库,可以手动将Step2里面下载的SDK,安装到引用的maven库中。用idea的话,刷新下图位置,就能引入到本地maven中。

			-	σ	)
-troomed and a communication of the second s	*=3	Maver	Projects		\$• ⊃!

或者通过IDEA的Module Settings,手动添加JWT-SDK本地jar包。

#### 😫 Project Structure

<b>\$</b>	<mark>+ –</mark> ტ	Name:	commons-io-2.4
Project Settings Project Modules Libraries Facets Artifacts Platform Settings SDKs Global Libraries	IIII commons-io-2.4         IIII Maven: ch.qos.logback:logback-classic:1.2.3         IIII Maven: com.fasterxml.jackson.core:jackson-annotations:2.9.10         IIII Maven: com.fasterxml.jackson.core:jackson-core:2.9.10         IIII Maven: com.fasterxml.jackson.core:jackson-core:2.9.10         IIII Maven: com.fasterxml.jackson.datatype:jackson-datatype-jdk8:2.9.10         IIII Maven: com.fasterxml.jackson.module:jackson-module-parameter-names:2.         IIII Maven: com.fasterxml:jackson.module:jackson-module-parameter-names:2.         IIII Maven: com.fasterxml:classmate:1.4.0         IIII Maven: com.jayway.jsonpath;json-path:2.4.0         IIII Maven: com.jayway.jsonpath;json-path:2.4.0	+ + ▼ ↓% C	ta − lasses C:\Users\hale\Downloads\JWT-SDK- C:\Users\hale\Downloads\JWT-SDK- C:\Users\hale\Downloads\JWT-SDK- C:\Users\hale\Downloads\JWT-SDK- C:\Users\hale\Downloads\JWT-SDK-
Problems	Image: Mayer: javax.annotation:javax.annotation-api:1.3.2         Mayer: javax.validation:validation-api:2.0.1.Final         Image: Javax.validation:validation: Javax.validation-api:2.0.1.Final         Image: Javax.validation: Javax.validati		

# 2.2. SAML 模板使用指南

## 一、概述

IDaaS平台支持基于标准SAML协议的SSO(Single Sign On 单点登录), IDaaS作为SAML协议中的 IDP(Identity Provider身份提供方)角色,提供用户的身份认证服务,用户可以登录一次就直接使用多个 SP(Service Provider 业务提供方)的服务,免去了每个应用都要登录的烦恼。

## 二、IDP发起和SP发起

SAML(Security Assertion Markup Language 安全断言标记语言)是一个基于XML的开源标准数据格式,为 在安全域间交换身份认证和授权数据,尤其是在IDP和SP之间。SAML是OASIS(Organization for the Advancement of Structured Information Standards 安全服务技术委员会)制定的标准,始于2001年,其 最新主要版本SAML 2.0于2005年发布。

作为一种流行的SSO协议, SAML同时支持IDP发起和SP发起, 也就是可以在登录门户后, 跳转到任意一个应用, 也可以从一个应用发起, 跳转到IDP, 登录认证后, 再跳转回这个应用, 继续SSO。二者都是SSO, 流程的前半部分参数不同, 后半部分是很相似的。

## 2.1、SAML的流程

### 2.1.1、SP发起SSO

用户请求SP资源,SP生成SAML请求,IDP接收并解析SAML请求并进行用户认证后返回SAML响应,SP接收并 解析SAML响应后,提起其中的令牌Assertion,提供被请求的资源给用户使用。



具体流程如下:

## 2.1.1.1、用户请求目标资源

用户向SP请求目标资源,例如目标资源为:

https://sp.example.com/myresource

SP会进行安全检查,如果SP已经存在有效的IDP安全会话上下文,则认为已经登录过,跳过步骤2~8。

## 2.1.1.2、重定向到IDP的SSO服务

SP会生成SAMLRequest,同时会把SP当前发起的URL生成一个随机数opaque,临时存放,同时把它作为RelayState,然后使用标准的HTTP 302重定向redirect到IDP的SSO服务,例如:

#### 302 Redirect

Location: http://idp4/enduser/api/application/plugin\_saml/<application\_id>/sp\_sso? SAMLRequest=xxx&RelayState=opaque

RelayState是SP的发起URL的不透明引用, SAMLRequest是Base64编码以后的<samlp:AuthnRequest>元素, <samlp:AuthnRequest>示例:

<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="identifier\_1" Version="2.0" IssueInstant="2004-12-05T09:21:59Z" AssertionConsumerServiceIndex="0"> <samls:sueInstant="2004-12-05T09:21:59Z" AssertionConsumerServiceIndex="0"> <saml:IssueInstant="2004-12-05T09:21:59Z" AssertionConsumerServiceIndex="0"> <saml:IssueInstant="2004-12-05T09:21:59Z" AssertionConsumerServiceIndex="0"> <saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"> <saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"></saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"></saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"</saml:IssuerServiceIndex="0"></saml:IssuerServiceI

如果需要的话, SAMLRequest还可以使用SigningKey进行签名。

## 2.1.1.3、浏览器转发SAML请求,重定向到IDP的SSO服务

浏览器将SP的SAMLRequest和RelayState通过一个GET请求转发到IDP的SSO服务:

GET /SAML2/SSO/Redirect?SAMLRequest=request&RelayState=opaque HTTP/1.1

Host: idp.example.org

## 2.1.1.4、IDP解析SAML请求

IDP解析SAML请求,通过Base64解码得到<samlp:AuthnRequest>元素。IDP会验证用户是否已经登录,如果已经登录则跳过步骤5。

## 2.1.1.5、认证用户

IDP认证用户身份,常用的方法是IDP返回登录页面给用户,IDP可以配置自己需要的认证方式,比如用户使用账号和密码进行登录认证。

## 2.1.1.6、用户认证成功后返回SAML响应

IDP认证用户身份以后会返回SAMLResponse响应,响应中包含如下表单:

```
<form method="post" action="https://sp.example.com/SAML2/SSO/POST" ...>
<input type="hidden" name="SAMLResponse" value="response" />
<input type="hidden" name="RelayState" value="opaque" />
...
<input type="submit" value="Submit" />
</form>
```

表单中的RelayState参数值就是步骤2中生成的RelayState, IDP会将其原封不动的返回。表单中的 SAMLResponse是Base64编码以后的<samlp:Response>元素, <samlp:Response>示例:

<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="identifier 2" InResponseTo="identifier\_1" Version="2.0" IssueInstant="2004-12-05T09:22:05Z" Destination="https://sp.example.com/SAML2/SSO/POST"> <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer> <samlp:Status> <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/> </samlp:Status> <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="identifier 3" Version="2.0" IssueInstant="2004-12-05T09:22:05Z"> <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer> <!-- a POSTed assertion MUST be signed --> <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature> <saml:Subject> <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"> 3f7b3dcf-1674-4ecd-92c8-1544f346baf8 </saml:NameID> <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <saml:SubjectConfirmationData InResponseTo="identifier\_1" Recipient="https://sp.example.com/SAML2/SSO/POST" NotOnOrAfter="2004-12-05T09:27:05Z"/> </saml:SubjectConfirmation> </saml:Subject> <saml:Conditions NotBefore="2004-12-05T09:17:05Z" NotOnOrAfter="2004-12-05T09:27:05Z"> <saml:AudienceRestriction> <saml:Audience>https://sp.example.com/SAML2</saml:Audience> </saml:AudienceRestriction> </saml:Conditions> <saml:AuthnStatement AuthnInstant="2004-12-05T09:22:00Z" SessionIndex="identifier\_3"> <saml:AuthnContext> <saml:AuthnContextClassRef> urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport </saml:AuthnContextClassRef> </saml:AuthnContext> </saml:AuthnStatement> </saml:Assertion> </samlp:Response>

这里重要的是Assertion部分,包含有用户的Subject身份信息。默认一般用IDP的私钥对整个 SAMLResponse 签名,也可以是对Assertion 签名,或是二者兼而有之,取决于IDP和SP的协商。

## 2.1.1.7、浏览器将SAML响应转发到SP的ACS

浏览器将SAMLResponse和RelayState以POST的方式转发到SP的ACS URL, SP继续解析令牌。

POST /SAML2/SSO/POST HTTP/1.1

Host: sp.example.com

Content-Type: application/x-www-form-urlencoded

Content-Length: nnn

SAMLResponse=response&RelayState=opaque

## 2.1.1.8、SP解析验证SAML响应

SP处理SAMLResponse响应, Base64解码得到<samlp:Response>元素,最重要的是要用SP中的公钥,来检查签名的合法性,如果合法,则抽取其中包含的用户信息Subject,找到对应的SP应用子账户,生成SP安全会话上下文。

## 2.1.1.9、用户获取目标资源

用户成功获取SP提供的目标资源。如果SP发现RelayState中有对应的URL,则提取这个URL,跳转到对应的URL。

## 2.1.2、IDP发起SSO

同上面的SP发起SSO不同, IDP发起可以实现用户登录IDP,在IDP中选择某个SP应用, IDP跳转到SP,用户使用SP的资源。



具体的流程如下:

## 2.1.2.1、用户访问IDP

用户打开IDP的登录页面。

## 2.1.2.2、用户登录IDP

使用配置好的如账号密码等方式登录到IDP。

## 2.1.2.3、用户选择需要的SP应用

#### 用户在IDP中选择需要使用的SP应用,背后会触

发https://xxxx.login.aliyunidaas.com/api/bff/v1.2/enduser/portal/sso/go\_0fbd26xxx? access\_token=9a2e8d41-cde9-4ba9-b09b-yyyy,继续流程。

## 2.1.2.4、IDP返回用户选择的SP应用的SAML响应

IDP生成用户选择的SP应用的SAMLResponse响应(前文已介绍),返回给用户的浏览器。

## 2.1.2.5、浏览器将SAML响应转发到SP的ACS

浏览器将SAMLResponse和RelayState以POST的方式转发到SP的ACS URL。

### 2.1.2.6、SP解析验证SAML响应

SP处理SAMLResponse响应, Base64解码得到<samlp:Response>元素,最重要的是要用SP中的公钥,来检查签名的合法性,如果合法,则抽取其中包含的用户信息Subject,找到对应的SP应用子账户,生成SP安全会话上下文。

注: 可以看到, 这一步和SP发起中的第8步非常类似, 包括下一步。

## 2.1.2.7、用户获取目标资源

自此,SSO结束,用户成功获取SP提供的目标资源。如果SP发现RelayState中有对应的URL,则提取这个URL,跳转到对应的URL。

### 2.1.2.8、显示目标资源

用户看到对应的应用目标资源。

### 2.2、SAML的Metadata

SAML协议中规定, IDP或SP的配置信息通过元数据(Metadata)信息实现, 配置过程只要交换IDP和SP的元数据配置信息就可以快速实现SSO配置。

## 2.2.1、IDP的Metadata

IDP的Metada是<md:EntityDescriptor>元素,示例如下:

<md:EntityDescriptor entityID="https://idp.example.org/SAML2" validUntil="2013-03-22T23:00:00Z" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<!-- insert ds:Signature element (omitted) -->

<!-- insert md:IDPSSODescriptor element (below) -->

<md:Organization>

<md:OrganizationName xml:lang="en">Some Non-profit Organization of New York</md:OrganizationNa me>

<md:OrganizationDisplayName xml:lang="en">Some Non-profit Organization</md:OrganizationDisplayN ame>

<md:OrganizationURL xml:lang="en">https://www.example.org/</md:OrganizationURL>

</md:Organization>

<md:ContactPerson contactType="technical">

<md:SurName>SAML Technical Support</md:SurName>

<md:EmailAddress>mailto:saml-support@example.org</md:EmailAddress>

</md:ContactPerson>

</md:EntityDescriptor>



标签	说明
entityID	IDP的唯一标识。
validUtil	元数据的过期时间。
ds:Signature	包含数字签名,以确保元数据的真实性和完整性。
md: Organization	组织信息。
md:ContactPerson	联系人信息。

IDP的SSO相关Metadata是<md:IDPSSODescriptor>元素,示例如下:

<md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"> <md:KeyDescriptor use="signing"> <ds:KeyInfo>...</ds:KeyInfo> </md:KeyDescriptor> <md:ArtifactResolutionService isDefault="true" index="0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://idp.example.org/SAML2/ArtifactResolution"/> <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat> <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat> <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://idp.example.org/SAML2/SSO/Redirect"/> <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://idp.example.org/SAML2/SSO/POST"/> <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://idp.example.org/SAML2/Artifact"/> <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" FriendlyName="eduPersonAffiliation"> <saml:AttributeValue>member</saml:AttributeValue> <saml:AttributeValue>student</saml:AttributeValue> <saml:AttributeValue>faculty</saml:AttributeValue> <saml:AttributeValue>employee</saml:AttributeValue> <saml:AttributeValue>staff</saml:AttributeValue> </saml:Attribute> </md:IDPSSODescriptor>

#### 主要元素信息为:

标签	说明
<md:keydescriptor use="signing"></md:keydescriptor>	IDP配置的一个私有SAML签名密钥和/或一个私有后端通 道TLS密钥。
<md:artifactresolutionservice>下的Binding</md:artifactresolutionservice>	SAML绑定信息。
<md:nameldformat></md:nameldformat>	SSO支持的SAML名称标识格式。
<md:singlesignonservice></md:singlesignonservice>	单点登录信息。
<saml:attribute></saml:attribute>	IDP提供的断言的属性。

## 2.2.2、SP的Metadata

SP的Metada是<md:EntityDescriptor>元素,示例如下:

<md:EntityDescriptor entityID="https://sp.example.com/SAML2" validUntil="2013-03-22T23:00:00Z"

xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"

xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<!-- insert ds:Signature element (omitted) -->

<!-- insert md:SPSSODescriptor element (see below) -->

<md:Organization>

<md:OrganizationName xml:lang="en">Some Commercial Vendor of California</md:OrganizationName> <md:OrganizationDisplayName xml:lang="en">Some Commercial Vendor</md:OrganizationDisplayName

>

<md:OrganizationURL xml:lang="en">https://www.example.com/</md:OrganizationURL>

</md:Organization>

<md:ContactPerson contactType="technical">

<md:SurName>SAML Technical Support</md:SurName>

<md:EmailAddress>mailto:saml-support@example.com</md:EmailAddress>

</md:ContactPerson>

</md:EntityDescriptor>

#### 主要元素信息为:

标签	说明
entityID	SP的唯一标识。
validUtil	元数据的过期时间。
ds: Signature	包含数字签名,以确保元数据的真实性和完整性。
md: Organization	组织信息。
md:ContactPerson	联系人信息。

SP的ACS相关Metadata是<md:SPSSODescriptor>元素,示例如下:

<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"> <md:KeyDescriptor use="signing"> <ds:KeyInfo>...</ds:KeyInfo> </md:KeyDescriptor> <md:KeyDescriptor use="encryption"> <ds:KeyInfo>...</ds:KeyInfo> </md:KeyDescriptor> <md:ArtifactResolutionService isDefault="true" index="0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://sp.example.com/SAML2/ArtifactResolution"/> <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat> <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat> <md:AssertionConsumerService isDefault="true" index="0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sp.example.com/SAML2/SSO/POST"/> <md:AssertionConsumerService index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://sp.example.com/SAML2/Artifact"/> <md:AttributeConsumingService isDefault="true" index="1"> <md:ServiceName xml:lang="en">Service Provider Portal</md:ServiceName> <md:RequestedAttribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1" FriendlyName="eduPersonAffiliation"> </md:RequestedAttribute> </md:AttributeConsumingService> </md:SPSSODescriptor>

标签	说明
<md:keydescriptor use="signing"></md:keydescriptor>	SP配置的一个私有SAML签名密钥和/或一个私有后端通 道TLS密钥。
<md:keydescriptor use="encryption"></md:keydescriptor>	SP公共SAML加密密钥。
<md:assertionconsumerservice>下的index</md:assertionconsumerservice>	<samlp:authnrequest>元素中的 AssertionConsumerServiceIndex属性的值。</samlp:authnrequest>
<md:assertionconsumerservice>下的Binding</md:assertionconsumerservice>	SAML的绑定信息。
<md:attributeconsumingservice></md:attributeconsumingservice>	lDP用来构造一个 <saml:attributestatement>元素,该 元素与Web浏览器SSO一起推送到SP。</saml:attributestatement>
<md:attributeconsumingservice>下的index</md:attributeconsumingservice>	SP在SSO时生成 <samlp:authnrequest>元素中 AttributeConsumingServiceIndex属性的值。</samlp:authnrequest>

## 三、IDaaS中配置SAML应用示例

IDaaS平台支持基于标准SAML协议的SSO,并提供来一系列的应用模版来方便配置,这里以阿里云RAM为例 演示如何配置。

### 3.1、获取SP的元数据信息

SP会提供自己的元数据信息,以阿里云RAM为例,登录控制台后找到元数据URL。

		Q 搜索文档、控制台、API、解决方案和资源	農用	工单	备宽	企业	支持	官网	<u>له</u>	F	1	简体	
RAM 访问控制	RAM 访问种制 / SSO 管理												
all in	cco 答理												
m.x	330 官庄												
	〇 阿里云支持器于 SAML 2.0 的 SSO (Single Sign On, 单点登录), 也称为身份联合登录。 阿思云用于中国支持器件 SSO 器器支援。												
用戶證	1. 通过角色 SSO、企业可以在本地 kiP 中管理员工信息,无需进行阿里云和企业 kiP 间的用户同步,企业员工将使用指定的 RAM 角色未登录阿里云												
用户	2. 通过用户 SSO,企业员工在登录局,将以 RAM 用户身份访问时提去。												
设置	角色 SSO 用户 SSO												
SSO 普弸													
权限管理 へ	SSO登录设置 ∠ 编辑												
援权	SSO 功能状态 开启												
权限策略管理													
	Annu ResearchinyLakaki Unit, https://signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/spinetadata.smittenanu/sint/signintaryunit.com/samu/samu/signintaryunit.com/samu/signintaryunit.com/samu/samu/samu/samu/samu/samu/samu/sam												
KAM 周巴言理													
OAuth 应用管理(公测中)													
													P
													2
													88

浏览器访问该URL得到元数据信息,显示如下:

This XML file does not appear to have any style information associated with it. The document tree is shown below

将上述内容可以导出,放在下一步使用。

## 3.2、IDaaS中配置SP的元数据信息

## 3.2.1、添加SP应用

准备好后, 接下来, 在IDaaS 中添加一个RAM应用。

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。

点击左侧导航栏 应用 > 添加应用

在右侧选择一个SAML应用,点击添加应用。IDaaS支持多种SAML应用,这里以添加阿里云RAM-用户SSO为例进行展示。

☰ (-) 阿里云						Q 讀素文档, 控制台.	API、解决方案和资源	壽用	工单 音:	5 企业	支持	官网	51 4	. A	٢	简体	٢
概流	添加应用																
快速入门	全部标准协会	议 定制模板															
<ul> <li>②用</li> <li>△</li> <li>○</li> <li>○<th>漆加5</th><th>立用 地会了所有已支持的可添加立 为两种:一种是支持标准的 JJ</th><th>用利表,管理员可以选择需要 NT、CAS、SAML等模板的S</th><th>1使用的应用进行初始化配置。 2用,在这里可以通过添加对</th><th>并开始后续使用。 应约后电应用模板来实现单应登录功能:另一种最定制的</th><th>立用,本美应用已经提供了</th><th>对接其单点登录或用户同</th><th>步的接口,由</th><th>IDaaS 为其括</th><th>供定制化模</th><th>板进行对接。</th><th></th><th></th><th></th><th></th><th></th><th>ĸ</th></li></ul>	漆加5	立用 地会了所有已支持的可添加立 为两种:一种是支持标准的 JJ	用利表,管理员可以选择需要 NT、CAS、SAML等模板的S	1使用的应用进行初始化配置。 2用,在这里可以通过添加对	并开始后续使用。 应约后电应用模板来实现单应登录功能:另一种最定制的	立用,本美应用已经提供了	对接其单点登录或用户同	步的接口,由	IDaaS 为其括	供定制化模	板进行对接。						ĸ
账户管理 分类管理	应用的标	应用名称	应用ID	标签	描述						应用	类型			操作		
认证 ^ 认证原	<b>C-</b> ]	阿里云RAM·用户SSO	plugin_aliyun	SSO, SAML, 阿里云	器于 SAML协议,实现由 IDaaS 单点登录到阿里云的 通过映射实现单点登录到RAM。	2刻台: 使用读模板, 需要	ERAM中为每个用户单独	创建RAM子则	(户, IDaaS)账	⊨¥0RAM <del>7</del>	账户 Web	应用			添加应	用	
RADIUS 证书管理	[-]	阿里云RAM-角色SSO	plugin_aliyun_role	SSO, SAML, 阿里云	基于 SAML 协议,实现由 IDaaS 单点登录到阿里云的 IDaaS账户和RAM角色通过转射实现单点登录到RAM	2制台:使用读模板,需要0 4。	RAM中创建RAM角色,不	需要为每个月	户单独创建R	M子账户,	Web	应用			源加应	用	
授权 ^ 权限系统	S	SAML	plugin_saml	SSO, SAML	SAML (Security Assertion Markup Language, 安全 (IDaaS) 和渦義方 (应用) 之间传递身份信息, 实 常广泛的运用。	新宣标记语言,版本 2.0) 昆基于网络跨域的单点登录	基于 XML 协议,使用包约 。SAML 协议是成熟的认	皆断直(Asse 证协议,在国	tion) 的安全 内外的公有云	》牌, 在接机 和私有云中。	」方 新非 Web	应用			添加应	用	
应用授权 审计 ~	W	WordPressSaml	plugin_wordpress_saml	SSO, SAML, CMS	WordPress 是全世界最初广泛使用的 CMS(Content 允许千万技术或非技术人员生产、管理各种类型的网 支持通过 SAML 协议单点登录到 WordPress 网站。	t Management System,内 站。从南亚网站、政府页面	容管理系统) 。它通过非 1到个人嫁客、主题论坛。	常强大的播作 WordPress P	家统和方便自 (支持的形式)	然的操作界 :常多样,IC	周, waaS Web	应用			添加应	用	
	M	阿里邮稿	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	建最和用户同步。					Web	应用			添加应	я	
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2										共5	<u>ج</u> (	1	1	) 彖/页 ~	跳至	1	I

点击添加SigningKey按钮,输入名称等信息,系统会据此生成应用的证书,私钥保留在IDP,公钥导出到 SP,用于IDP和SP通信的签名验签。

添加应用(阿里云RAM-用F	⊐SSO)						$\times$
导入SigningKey 🍒	边[SigningKey						
别名	序列号		有效期	秘钥算法	算法长度	操作	
		暂无数据					

如果没有现成的证书可以选择,则填写以下信息生成一个,其中的名称信息最好是和这个应用比如RAM关联的,方便将来识别。

 $\times$ 

法加Signir	nakev
நடிப்புகாடா	iyixey

*名称	请输入名称	
部门名称	请输入部门名称	
公司名称	请输入公司名称	
*国家	请选择	$\sim$
* 省份	请输入省份	
城市	请输入城市	
*证书长度	请选择	~
*有效期	请选择	$\sim$
	提交取消	

### 无论是选择已有的还是刚添加的,找到对应的SigningKey,选择它。

添加应用(阿里云RAM-用户SSO)									
导入SigningKey 添加SigningKey									
别名	序列号	有效期	秘钥算法	算法长度	操作				
CN=试用公司, ST=BJ, C=CN	1037460220135891327	365	RSA	2048	选择导出				

接下来要填写更多的应用信息,名称等信息可以自定义,Entityld、ACS URL等信息从步骤1中的到的SP的元数据中复制过来,需要填写的主要信息如下:

参数名称	说明
应用名称	所添加应用的名称,可以为任意值,但最好和应用相关。
应用类型	引用的类型,只有选中的应用类型才会在用户对应客户端 中显示。
IDaaS Entityld	在IDaaS中设置的认证参数,需要将此参数配置到SP中, 在IDaaS导出的 metadata 里可以获取,例如 https://signin.aliyun.com/117xxxxxxxxx63/saml/S SO。

SP Entity ID	在SP中设置的Entity ID,需要复制到IDaaS的配置中, 可 以在RAM的metadata中获取, 例 如https://signin.aliyun.com/117yyyyyyyyyy63/saml /SSO。
SP ACS URL (SSO Location)	单点登录地址,这里以阿里云RAM为 例:https://signin.aliyun.com/saml/SSO。
NameldFormat	名称标识格式类型,这里以阿里云RAM为例,选择 urn:oasis:names:tc:SAML:2.0:nameid- format:persistent。

添加应用 (阿里)	云RAM-用户SSO) ×
图标	<b>[</b> -]
	<ul> <li>④ 上传文件</li> <li>图片大小不超过1MB</li> </ul>
应用ID	scheinigeringen without &
SigningKey	1aefae1073afde6cf629d2224bb0f6f1AJSLFIFpeZe
*应用省称	026-JH-MANAEM
安全等级	5 ~ * * * * * * * * * * * * * * * * * *
相延认业力式	当用户安全级别低于应用需求时,请用此处指定的方式进行强化认证。
*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	请输入阿里云个人城名
125	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
	1元,: IILUp-X/Siginii.anyun.com/10441940000/1062/Saliii/SSO, 共平10441940000/1062/パーへ成石成一即辺内石。
*SP Entity ID	请输LASP 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	<del>此项不能为交</del> 法論入SP ACS URL(SSO Location)
URL(SSO Location)	默认地址是 https://signin.aliyun.com/saml/SSO。 此项不能为空
*RelayState	请输入RelayState
	登录成功后阿里云跳转地址, 以http或https开头。 此项不能为空
*阿里云 AccessKeyID	请输入AccessKeyID
	ACCessKeyIU用于进行数据问步,右需要使用问步功能请填与。
阿里云 AccessKeySecr et	请输入AccessKeySecret AccessKeySecret用于进行数据同步,若需要使用同步功能请填写。
* NameldFormat	um accie namester SAMI 2 Ornamaid format transiant
*NameroFormat	
*Binding	POST ~ *
Sign Assertion	
*账户关联方式	○账户天既(系统按王士账户对应大系进行主动天联,用户添加后需要管理员审批) ○账户缺时(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)
	<b>提父</b>

填写完成后提交保存,如果应用是禁用状态,可以继续修改重新提交。

## 3.2.2、启用应用并且授权

应用配置好以后需要先启用应用,并且将服务授权给一个账户,点击左侧导航栏 **应用 > 应用列表** 启用该应 用并授权给账户。

#### 单点登录配置·标准协议模板使用指南

#### 应用身份服务

					Q 搜索文档、控制台、AP	、 熊: 義用 工単	音変 企业 支持 首同 四 🗘 🖓 🕐 简体 📑
概范	应用列表						海加級用
快速入门	☆      应用     当済	列赛 员可以在当前页面管理已经添加的所有应用,应用 10时应用后,应该确认应用处于启用状态,并已经3	可以实现 <b>单点登录和意调明多能力。</b> 地质了接权。在应用并播中,可以看到应用的详细信息、单点登录地址、子张户配置。	同步配置、授权、审计等信息。			×
添加应用	请输入应用;	称		Q			
账户 ^ 和約万组	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
账户管理	C-)	阿里云RAM-用户SSO	idaas-on-hangzhou-vr533mky3c3plugin_allyun	Web应用			援权 详情 ~
30英吉地 认证 ^ 以证原 RADIUS 证书管理 指約 ^							共1条 < 1 > 10条页~ 載至 1 页
权限系统 应用授权							
审计 ✓ 其它管理 ✓ 公局 ✓							
va							

#### IDaaS支持多种方式进行授权,这里以按应用授权账户为例。

			Q	搜索文档、控制台、API、编注 费用 工单 备案 企业 支持	🕴 宮同 🖸 🗘 🗑 箇体 📑
概范	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 按账户援权应用	按应用授权账户 按分类授权应用			
应用 ^ 应用列表	应用(1)	账户数 (5) 已损权(0)个			
添加应用	諸編入应用名称进行直找 Q	请输入账户名称进行查找			۹.
账户 个	间理云RAM-用户SSO	> 账户名称	显示名称	邮箱	
机构及组	#18 ( ]	a zhaoliu	赵六	zhaoliu@abc.com	
<b>床</b> 戸宮垣 分栄管理		<ul> <li>wangwu</li> </ul>	王五	wangwu@abc.com	
认证 ^		isi isi	李四	lisi@abc.com	
认证原		zhangsan	张三	zhangsan@abc.com	
RADIUS		idaas_manager	默认管理员	manager@idaas.com	
证书管理				#	5条 < 1 > 龍至 1 页
权限系统		9847			
应用授权					
审计 、					
其它管理 💙 🗸					
设置					
					P
					BS

保存后,这个用户登录就可以看到这个应用了。

### 3.2.3、IDP新建子账户(非必须步骤)

一个系统要SSO到另外一个系统,需要使用对方能够识别的子账号进行认证,往往登录到IDP的主账户和应用 SP的子账户是不一样的,可以使用账号同步(两套系统中的账号信息相同)或者新建子账户进行账号映射的 方法。账号映射是指给IDP的账户建立一个SP中已经存在的账户作为子账户,身份认证的时候通过子账户进 行认证。例如SP系统中有个账户"demo",我们想用IDP系统中的"zhangsan"账号SSO到SP,则需要给账 号"zhangsan"新建一个对应的子账户"demo"。这里以阿里云RAM演示新建子账户的功能,如下图,阿 里云RAM中有账户demo@117yyyyyyyy63.onaliyun.com。

#### 应用身份服务

		○ 除于文档 种新会 API 能动力型的密度 ■用 丁腈 每天 合伙	रुक्त हल जि. पूर्व क्रिक क्रिक क्रिक
RAM 访问控制	RAM 访問绘制 / 用户		
概范	用户		
人员管理 ^ 用户组	● RAM用户是一个身份实法,它遵承代表思幼组织中美要访问开放男幼儿员成应用程序。 建始如果作步骤如下: 1.创建用户,并为用户少数已就是表示符(用户是更地给估装备)或创建 Access(ary (应用程序清明 API 站员)。 		
用户	2.00000-9100-1010(10000-1001-9000)00-1001000(0)。		C
SSO 管理	□ 用户登录名称/显示名称 餐注	创建时间	操作
权限管理 ^	demo@117. ● //▲ 1-963.onaliyun.com demo	2020年9月24日 09:07:35	添加到用户组 添加权限 制脉
RAUA 化同原素器管理 RAUA 角色管理 CAuth 应用管理(公测中)	i Kanshiri-ni Kandori		
			E F 8

IDaaS中新建子账户有两种方式,操作如下:

## 3.2.3.1、授权账号新建子账户

登录授权账户,点击左侧导航栏 **主导航 > 应用子账户**添加应用子账户功能中提交新建子账户申请。由于上一步阿里云RAM中的账户是demo@117yyyyyyyy63.onaliyun.com,所以这里子账户的名称应该填 demo。IDaaS在SSO的时候,会将子账户(demo)和步骤3.2.1中配置的阿里云个人域名 (117yyyyyyyyyy63.onaliyun.com)进行拼接映射到阿里云RAM的账户。

IDaaS统—认证身份平台				添加子账户		
欢迎 · IDaa S	应用子账户			选择应用	阿重云RAM·用户SSO	
	子账户列表 子账户审批				時活得失能的应用	
应用管理	<b>派加这用于账户</b> 建愈合用名称		۹	主账号	zhangsan	
	应用图标 应用名称	审批状态	主账户	子账号	demo	
我的账户二次认证	C-D 阿里云RAM-用户SSO	Bāt	zhangsan		提示此应用子账户采用的是 <b>账户映刻</b> 方式。系统会侦照应用配置的账户关款缺划字在作为主键登录到 应用系统。	
我的满意					007	
					—	
	◎ IDaaS 浙ICP曾12022327号					

登录管理员账户,点击左侧导航栏其它管理 > 审批中心 审核通过该应用子账户的添加。

### 单点登录配置·标准协议模板使用指南

								Q 撞震文档, 控制台	、API、解决方面和注	费用 工单	晉宽 企	业支持背	in d	₩ ®	简体 📑
概范	审批中心 VIP														
快速入门	子账户审批 注册审	批													
应用 ^															
应用列表 语***中国	审批中心	IDaaS 系统中管理员集中州	理所有需要审批内容的功能	<b>亦置,当有待审教项</b> 州到	101、会在左侧圆舷栏4	相应位置有数字气流程示。									×
NAULUZ/H	✓ 子账户指的题 审批通过后。	量单点登录时带给应用的身份 用户将可以使用子账户单。	0标识。如果某应用设置其 19登录到应用系统中,请确	主子账户缺财关系为「账 人IDaaS 用户主账户和于	产关联]时,用户在装 「账户的对应关系后完!	上试单点登录的时候,如果》 成审批。	Q有子账户,则会提交一	个子账户绑定申请。由管理员	在此处进行审批。						
机构及组					_										
账户管理		子账户		待审批	~ 沈広	重量									
分类管理	主账户 (申请人)		子账户		应用名称		申请	时间		审批状态			操作		
以业 ^ 认证原	zhangsan		demo		阿里云RA	M-用户SSO	2020	0-12-08 11:22:29		待审批			查看详情 审批	快速同意快速	書拒绝
RADIUS															
证书管理												д	1張 < 1	> 965	1 页
授权 へ 权限系统															
应用授权															
审计 ~															
其它管理															
申試中心															
消息管理															
会活管理															88
教的消息 5															•
0.B															
子账户审	批														$\times$
- /00															
应用名称	k:	阿里云RA	M-用户SS	O											
12012011															
应用名称	F:	demo													
	-	2020 42 0	0 44-00-00												
申请的旧	1:	2020-12-0	08 11.ZZ.Z9												
宙北音口	η.	诸蝓λ宙	拙意见												
H MARN		appendy Corr													
															1
		同意	拒绝												

## 3.2.3.2、管理员新建子账户

管理员新建子账户不需要审核过程,具体操作为:

登录管理员账户,点击左侧导航栏 应用 > 应用列表 找到添加的应用,点击详情中的查看应用子账户。

■ (•) 阿里云			Q 操家文档、控制台、API、解决方面	易用 王单 發素 企业支持 官同 🖸 🗘 🗑 简体 🄮
构近	应用列表			泽加盘用
快速入门 应用 ^	血用利果     章 管理同时以在当前范围管理已经添加的所有应用。应用可以实现单位管理     当该加利应用后,应用等以实现单位管理     正有利以实现单位管理     正有利以实现单位管理     日本時以应用处于由用状态,并已经完成了使权。在应     日本     日本	和激調明步能力。 用洋橋中,可以看到应用的洋垢信息、单点登录地址、子孫戶配置,同步配置。	援权、审计等信息。	×
添加应用	请输入应用名称	<u>م</u>		
账户 ^ 机构及组	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
账户管理	C-D 阿里云RAM-用户SSO	idaas-cn-hangzhou-vr533mky3c3plugin_allyun Web应		● 授权 详确 ▲
分类管理 认证 へ 1157項	应用信息	认证信息	账户信息 - 同步	账户信息 - 子账户
RADIUS 证书管理	应用的详细信息 重新详编 师改应用 题外应用	应用的单点登录地址 IDaaS发起地址	SCIM协议设置以及悲煽使机构。相同步推送至应用 同步机构 SCIM配置	平台主张户与运用系统中子张户的关联表 <b>查着应用子张户</b>
授权 ^ 权限系统	授权信息	审计信息	API	普選疫用内权限
应用授权	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	管理应用内莱单与功能权限
₩÷ ~	授权	查看日志 查看同步记录	API Key API Secret	绑定权限系统
142回道 ~ 142回道 ~				共1条 < 1 > 10条页> 副至 1 页
				8

## 点击添加账户关联,添加子账户。

	E						Q 撤款文档, 控制台, API, 解决方言	調用 工单 智雲 企业	支持 官网 四	0. A Q	简体 🚮	
概范		应用列表 / 子账户										
快速入门		← 子账户							添加账户关联	批星导入	批量导出	
应用 <u>应用列表</u> 添加应用 账户		子账户 子账户箱的是在测空应用系 举例: IDaaS 中有主账户 3 账户关联方式:在应用值题	S版中,用户会以什么身份进行访问。 张三(用户名 zhangsan),在企业的 如果选择了账户缺款,即款认主	主账户指的是 IDaaS 中的账户。在进行者 BPM 应用系统中,这个用户的用户名量 账户和子贩户完全一致,无器配置。如果	1.总登录时,IDaaS 会向应用系统传递 agoodman,即子张户应为 agoodma 选择了账户关款,则需要在这里进行:	brize的子账户,读子账户需要在应用系的 n,与主账户 zhangsan 进行关联。 事动的子账户做漏和主子账户关联。	克中存在且可 <b>计别。</b>				×	
机构及组 账户管理		同里云RAM.用户SSO										
分类管理		主账户 (账户名称)				Q						
い 正海 の 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	^	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		
RADIUS		zhangsan	张三	demo	无	已关题	已通过	2020-12-25		制除		
证书管理									共1条 ( 1	> 跳至	1 页	
授权 权限系统	^											
应用授权												
审计	Ň											
與已8年 设置												
											88	
												ļ

## 输入授权账户(主账户)和子账户,点击保存完成子账户添加。

≡ (-) 阿里	6						Q HES	的文档、控制台、API、解决方面	勝用 王单 發雲	企业 支持	官河 🖾	0" W	1) (C) (C) (C) (C) (C) (C) (C) (C) (C) (C	-
板近		应用列表 / 子凱卢					添加账户关联							×
快速入门		← 子账户												
应用	~						* 王珠尸							
应用列表		子账户 ② 子账户描的是在描述应用系统中	·, 用户会以什么身份进行访问。主账户打	i的是 IDaaS 中的账户,在进行单点整要	时,iDaaS 会向应用系统传递对应的子辨	沪,读子账户需要在应用	*子账户	子账户						
NALLWAS		▼ 準例: IDaaS 中有主账户张三 账户关联方式: 在应用创建时,	(用户名 zhangsan) , 在企业的 BPM 应 如果选择了账户缺制,即默认主账户和引	用系统中,这个用户的用户名易 agoodm 一般户完全一致,无需配置,如果选择了新	ian,即子账户应为 agoodman,与主账户 制户关联,则需要在这里进行手助的子账。	P zhangsan 进行关联。 户创建和主子账户关联。		保存 返回						
机构及组														
账户管理		PER 22 (174m-19)-330												
分类管理					۹									
认证		账户名称	显示名称	子账户	子账户密码	是否关联								
RADIUS		zhangsan	*E	demo	无	EXR								
证书管理														
授权														
应用授权														
审计														
其它管理。														
设置														

## 3.3、SP中配置IDaaS的元数据信息

## 3.3.1、获取IDaaS的元数据信息

以IT管理员账号登录云盾IDaaS管理平台,点击左侧导航栏 **应用 > 应用列表**选择刚才添加的应用,点击查看 详情,如下图:

三 (-)阿里云			Q 搜索	文档、控制台、API、 解注	费用 工单 晉宮 企业 支持	直网 🖸 🗘 🗑 🗑 简体 🃑
概范	应用列表					泽加应用
快速入门						×
应用 ^ 应用列表	○ 加利利義 管理员可以在当前页面管理已经添加的所有应用,应用可以实现单点微量利 当添加购应用后,应该确认应用处于局用状态,并已经完成了接权。在应用	( <b>政務同</b> 步能力。 1)洋橋中,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、1	授权、审计等信息。			
添加应用	请输入应用名称		a.			
账户 个 机构及组	应用图标 应用名称	应用10 设备	6类型	应用状态	二次认证状态	操作
账户管理 分类管理	「回量云RAM-用户SSO	idaas-cn-hangzhou-vr533mky3c3plugin_allyun Wel	b应用			授权 详情 •
认证 ^	应用信息	认证信息	账户信息 - 同步		账户信息 - 子账户	
认证原	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、组同步推送至应用		平台主账户与应用系统中子账户的关键	民族
RADIUS 证书管理	<b>查看详情</b> 修改应用 删除应用	IDaeS发起地址	同步机构 SCIM配置		查看应用子账户	
援权 个	援权信息	审计信息	API		管理应用内权限	
权限系统	应用与人员组织的规权关系	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	
<u></u> 一用技权	接权	查看日志 查看同步记录	API Key API Secret		绑定权限系统	
■FT - 其它管理 ~ 没重 ~					共1条 ∢	1 > 10 泉页 ~ 第至 1 页
						8

点击导出SAML元配置文件,将IDaaS的元数据文件保存到本地电脑。

应用详情 (阿里云RAM-用户SSO)

应用图标	<b>C-</b> J
应用ID	idaas-cn-hangzhou-vr533mky3c3plugin_aliyun
应用名称	阿里云RAM-用户SSO
SigningKey	2fef4d24a967c66dc8a85544ed9e987d7RSqU02gvA8
NameldFormat	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
阿里云个人域名称	117 🛶 1736 😹 150 63.onaliyun.com
SP ACS URL(SSO Location)	https://signin.aliyun.com/saml/SSO
IDaaS IdentityId	https://signin.aliyun.com/117/21、102/1003/saml/SSC 导出 IDaaS SAML 元配置文件
账户同步地址	/api/application/aliyun/account/3e625fc2316302cb74eaec0ed2b7cfefBDLh2qPiGHQ
SP Entity ID	https://signin.aliyun.com/117%: % P#0# 1#0#3/saml/SSO
Binding	POST
Sign Assertion	无
RelayState	无
AccessKeyID	无
AccessKeySecret	无

IDaaS元配置文件示例如下:

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://signin.aliyun.c om/117xxxxxxxx63/saml/SSO">

<md:IDPSSODescriptor WantAuthnRequestsSigned="false" protocolSupportEnumeration="urn:oasis:name s:tc:SAML:2.0:protocol">

<md:KeyDescriptor use="signing">

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:X509Data>

<ds:X509Certificate>TIIC4jCCAcqgAwIBAgIIDmXMktHMYX8wDQYJKoZIhvcNAQEFBQAwMTELMAkGA1UEBhMC Q04xCzAJBgNVBAgTAkJKMRUwEwYDVQQDDAzor5XnlKjlhazlj7gwHhcNMjAxMjA3MDMwNTU3WhcNMjExMjA3 MDMwNTU3WjAxMQswCQYDVQQGEwJDTjELMAkGA1UECBMCQkoxFTATBgNVBAMMDOivleeUqOWFrOWPuD CCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALiuwcn+sbMaVRT2Byb3GzBV1P0eOoK326fQS9rdea GalykSMqCMMKOZ+/QfdMWh+9Fr59A5pIEbCN7aP3P+cV1ClqhfKD4DTbsmGikSiUYgYf4tWztZx9NFWyuoucm8 LOKKpKIPbjUyLudzLlQGOCrX/4Be0md4mIVZMK96J41jRuJXUTxFepE0cTEi15SXbEsXrnJ1wueFylNKl9JerbCJ1 EDayktAYvkMrmn2d2R2etiVR4Una9pBqtPvCEIPKCNesWAE/3AcWTgSj+u8ocnTgnknIfVO65QRxaNrDAyTOpkq uXFshs+DtlILEdk2p9UUxkUCNySbIIM/gVgL0TkCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAeDdH7BYcalDYfpN KvJrHA9rKZ2vBTi4uy2WoXcIE0EdzBGUC41oPL5g3ictNA+4S8tnCkzl8aQr79tjUmcL/0Uzv4sdOggwglmkgw3kek 9Yq44i/ycMN8HVeF/vtyVxhlvqBeXU2P5n6jFqatG+VkeVGyiJQHwuP1UHokXWwyukcjr35CQQX5WALFNJ+F68IC KT9Ulqb5GtQgrd1JoRQB1Eb//IjxlZJAvZ6CxLnVCgVUSOI4xYEb8ATZPbzLIMIyXN4U6r6VxvBJuW/eMcqogYSYss bngSgpHmZFV9+MrDSjJLLtsVRuzmF+cBisojvo53z3EiNu/c4FGlUuKozPA==</ds:X509Certificate> </ds:X509Data>

</ds:X509Data

</ds:KeyInfo> </md:KeyDescriptor>

<md:KeyDescriptor use="encryption">

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

<ds:X509Data>

<ds:X509Certificate>TIIC4jCCAcqgAwIBAgIIDmXMktHMYX8wDQYJKoZIhvcNAQEFBQAwMTELMAkGA1UEBhMC Q04xCzAJBgNVBAgTAkJKMRUwEwYDVQQDDAzor5XnlKjlhazlj7gwHhcNMjAxMjA3MDMwNTU3WhcNMjExMjA3 MDMwNTU3WjAxMQswCQYDVQQGEwJDTjELMAkGA1UECBMCQkoxFTATBgNVBAMMDOivleeUqOWFrOWPuD CCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALiuwcn+sbMaVRT2Byb3GzBV1P0eOoK326fQS9rdea GalykSMqCMMKOZ+/QfdMWh+9Fr59A5pIEbCN7aP3P+cV1ClqhfKD4DTbsmGikSiUYgYf4tWztZx9NFWyuoucm8 LOKKpKIPbjUyLudzLlQGOCrX/4Be0md4mIVZMK96J41jRuJXUTxFepE0cTEi15SXbEsXrnJ1wueFylNKl9JerbCJ1 EDayktAYvkMrmn2d2R2etiVR4Una9pBqtPvCEIPKCNesWAE/3AcWTgSj+u8ocnTgnknlfVO65QRxaNrDAyTOpkq uXFshs+DtlILEdk2p9UUxkUCNySbIIM/gVgL0TkCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAeDdH7BYcalDYfpN KvJrHA9rKZ2vBTi4uy2WoXcIE0EdzBGUC41oPL5g3ictNA+4S8tnCkzl8aQr79tjUmcL/0Uzv4sdOggwgImkgw3kek 9Yq44i/ycMN8HVeF/vtyVxhlvqBeXU2P5n6jFqatG+VkeVGyiJQHwuP1UHokXWwyukcjr35CQQX5WALFNJ+F68IC KT9Ulqb5GtQgrd1JoRQB1Eb//IjxlZJAvZ6CxLnVCgVUSOI4xYEb8ATZPbzLIMIyXN4U6r6VxvBJuW/eMcqogYSYss bngSgpHmZFV9+MrDSjJLLtsVRuzmF+cBisojvo53z3EiNu/c4FGlUuKozPA==</ds:X509Certificate> </ds:X509Data>

</ds:KeyInfo>

</md:KeyDescriptor>

<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https: //lidcfkpjfb.login.aliyunidaas.com/enduser/api/application/plugin\_aliyun/idaas-cn-hangzhou-vr533mky3c3p lugin\_aliyun/sp\_sso"/>

<md:SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://li dcfkpjfb.login.aliyunidaas.com/enduser/api/application/plugin\_aliyun/idaas-cn-hangzhou-vr533mky3c3plu gin\_aliyun/sp\_sso\_post"/>

</md:IDPSSODescriptor>

</md:EntityDescriptor>

## 3.3.2、SP中配置元数据信息

不同的SP配置IDP的元数据方式不同,有的需要填入参数,有的可以直接上传元数据文件。以阿里云RAM为例,在阿里云RAM选择开启SSO功能,并且上传刚刚下载的元配置文件,完成SP中的IDP元数据信息配置。

#### 应用身份服务

☰ (-) 阿里云		Q 搜索文档, 控制台, API, 解决方案和资	滚 義用	工単	晉宮 企业	支持 官	9 22	٥.	₩ @	简体	٢
RAM 访问控制	RAM 编阅绘制 / SSO 世现		编辑 SSG	) 登录设	置						×
<b>6</b> .2	SSO 管理		SSO 功能状t	5.0							
人気変変 ^ 用い地 用い地 空音 SSD 管理 SSD 管理 系現管理 ^ 現代 名词無地管理	P 開設改体部等 SAM 20 的 SSO (Single Sign On, 单独建築), 合物力學的發展量為, 開設な紙を加約時期 SSO 自然力式, 通知用 SSO 自然力式, 金融 SSO 自然力式, 金融 SSO 自然力式, 金融 SSO 自然力式, 金融 SSO 自然力式, 金融 SSO 自然力, 金融 SSO 自然力, 金融 SSO 自然力, 金融 SSO 自然的, 金融 SSO 自然的, 金融 SSO 自然的, 金融 SSO 自然的, SSO 自然の, SSO 自然的, SSO 自然的,		<ul> <li>开启</li> <li>元数据文档。</li> <li>上校文件</li> <li>通勤域名 @</li> <li>开启 (</li> <li>设置域别名 E</li> </ul>	<ul> <li>关闭</li> <li>●</li> <li>●</li> <li>关闭</li> <li>●</li> <li>●</li> <li>关闭</li> </ul>	屬較能后,SSC	) 辅助城名将会失	22				
RAM 角色管理 CAuth 应用管理 (公则中)	< MICHER										
			<b>8</b> 2	关闭							

## 3.4、功能演示

## 3.4.1、IDP发起SSO

配置完成后, 就可以检查结果了。授权用户登录IDaaS, 点击左侧导航栏 **主导航 > 首页** 在我的应用中点击 该应用进行单点登录, 点击应用的图标进行单点登录。

IDaaS统一认证身份平台	ä. 
欢迎·IDaaS	我的应用
<b>主导航</b> ^	Web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 我的日志	て 「 の 里 云 RAM-用 户 SSO 移 动 広用
	当前没有授权的移动应用。

选择子账户demo进行单点登录。

请选择一个应用子账户	
由于你在该应用中关联了多个子账户,所以需要选择一个子账户	
zhangsan	
demo	

成功登录阿里云RAM控制台,然后就可以看到阿里云作为SP提供的资源了。

∃ (-)阿里云			
您好, demo			
运维管理 × 产品与服务	务 × 新建页面 +		
资源预警 ⑦			安全预警
近24小时报警 0	严重事件概览 0	警告事件概览 O	安全评分 ⑦         告答           95/100         0
ECS 实例负载正常			① 云产品风险监测 ⑦ 去授权
			. SSL 证书 ⑦ 去配置
			🦺 Web入侵检测 ⑦ 免费检测
常用导航			Q 搜索

如果账号配置错误或者选择的登录账号不是阿里云RAM中的账户,则会提示账户不存在。



## 3.4.2、SP发起SSO

同样,正确配置后,也支持SP发起,首先找到阿里云RAM子账户登录地址。

☰ (-) 阿里云				Q 證書文档, 拉制台, API, 解釋	約方當和资源	專用 工单 督室 企业 支持	in [1] (1]	D ata 🧐
RAM 访问控制	RAM 访问控制 / 概范							
概范	● 参与访问控制易用性问卷	反讀,协助我们提升严品体验。						
人员管理 へ	我的账号					账号管理		
用户组	用户	用户组	自定义策略	RAM 角色		子甩户		
用户	1/1000	1 / 50	0 / 1500	0/1000		用户登录地址	and a second and a local data of a second	
设置						编程默认成名	ionalyun.com/login.ntm 급 受制	1
SSO 管理	安全检查							
权限管理 へ	> 主账号开启MFA (多因	<b>東</b> 认证)		•	<b>未完成</b>	快速入口		
授权	> 子用户秘钥蛇转				已完成	创建用户组	创建用户	
◎ ○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	> 使用子用户进行日常工	ite			已完成	添加权限	创建自定义策略	i -
RAM 用色管理	> 创建用户组进行授权				已完成	创建 RAM 角色	修改 RAM 用户安全	設置
CAULY WHEN (2004)	> 创建自定义权限策略			•	未完成			
	> 为子用户启用MFA				) 未完成			
	土下载安全报告 🛛 土下载	用户凭证报告 NEW 💡						
								E?
								88

贴到浏览器跳转后, 登录界面上可以看到"主账号登录"和"使用企业账号登录"两种选择。主账号登录是 使用阿里云RAM自己的账号和密码进行登录,点击使用企业账号登录,则开始进行IDaaS的SSO过程。

<b>[-] 阿里云</b> RAM 用户登录		简体 阿里云首页
	主称号建杂	
	使用企业账号器券	
	下载词里云 App 開	
	RAM 用户登录码里云 App,随时推动修动管控	
阿里巴巴集团 1	688 全球進業通 淘宝网 天道 駅划算 一海 阿里妈妈 阿里云计算 YunOS 万网 支付宝 来4 © 2009-2020 Aliyun.com 版初所有 増価电信/送発受置许可证: 新 82-20080101	ž
	۵	

浏览器会自动跳转到IDP的登录界面,登录IDaaS授权账号,例如zhangsan,然后IDaaS认证完成以后,找到 对应的子账号,生成SAMLResponse,就会跳转到阿里云RAM控制台。

				X
		回転 ひんしん (単本) (第二) (第二) (第二) (第二) (第二) (第二) (第二) (第二		<u>A</u>
		图495 1月48入3金证49	-E17,M) 忘记虑吗?	
	/	Ğ₹		

自此, IDP发起和SP发起全部工作正常!

## 四、FAQ

## 4.1、代码中如何解析SAMLRequest

SP发起SSO的时候会生成SAMLRequest, SAMLRequest是Base64编码后的内容,我们需要解析以后才能得 到需要的内容,如下代码可以解析SAMLRequest,然后就可以拿到AuthnRequest进行认证。 import java.io.\*;

import org.opensaml.xml.util.Base64;

import java.util.zip.InflaterInputStream;

import java.util.zip.Inflater;

public class SamlRequestTest {

public static void main(String[] args) throws Exception {

// 接收到的原始SAMLRequest

String samlRequest = "fZJNT%2BMwElbv%2Bysi3%2FNhd9umVhPUXYQWiRUVCRy4IMedFIMzzmacavvvC Qll4bAcfLD0fnjm8frsb2ODA3RkHGaMRwkLALXbGdxn7La8CFN2ln9bk2qsaOWm9494A396IB9siKDzg%2B%2Bn Q%2Bob6AroDkbD7c1Vxh69b0nGMZk9GoyUNccel%2B2a%2BDUqLoprFpwPKQaVH6tPBmyttmiPhyqybv9uN TulaPQD7vqhOFatGU5rjR4T4tb2g%2FxhksejPtQYVmCehmHC2h3h%2BETPz%2B3yk5LH1D4QORZcuE7DOGH GamUJWHB5njElaljCTOxTriuuVlzVS6iTNIVK8F01iGiriMwB%2FtmlerhE8gp9xkQikpCLMElLzuV8JvkqWqTf71m w7Zx32tkfBqeF9x1Kp8iQRNUASa9lsfl9JUWUyGoSkfxVlttwe12ULLg7gR0v4AaUSHJC9XVW%2B1bM8omsHF% 2FcfUz4OkCd2LP8%2F6R5ukgWq8V8NpsnKyEW7%2BjX8cfW%2FO36%2BXvlLw%3D%3D&RelayState=https %3A%2F%2Fhomenew.console.aliyun.com%2Fhome%2Fscene%2FOperation";

#### // base64解码

byte[] decodedBytes = Base64.decode(java.net.URLDecoder.decode(samlRequest, "utf-8")); // 获取输入流

ByteArrayInputStream byteArrayInputStream = new ByteArrayInputStream(decodedBytes);

InflaterInputStream inflaterInputStream = new InflaterInputStream(byteArrayInputStream, new Inflater (true));

```
byte[] buffer = new byte[decodedBytes.length];
ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream();
//信息写到输出流
for (int i = 0; i != -1; i = inflaterInputStream.read(buffer)) {
    byteArrayOutputStream.write(buffer, 0, i);
    }
String result = new String(byteArrayOutputStream.toByteArray(), "UTF-8");
    //输出解析后结果
    System.out.println(result);
  }
}
```

解析后的结果为

```
<?xml version="1.0" encoding="UTF-8"?>
```

<saml2p:AuthnRequest AssertionConsumerServiceURL="https://signin.aliyun.com/saml/SSO" Destination= "https://nplclnlyvb.login.aliyunidaas.com/enduser/api/application/plugin\_aliyun/idaas-cn-beijing-foyeyjskk p7plugin\_aliyun1/sp\_sso" ForceAuthn="false" ID="a2fe7e32g81cb1a91af7ef088eb21db" IsPassive="false" Is sueInstant="2020-12-08T11:53:19.684Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POS T" Version="2.0" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"><saml2:Issuer xmlns:saml2="urn:o asis:names:tc:SAML:2.0:assertion">https://signin.aliyun.com/1860696533509226/saml/SSO</saml2:Issuer></saml2p:AuthnRequest>

# 2.3. OAuth2.0模板使用指南

### 概述

IDaaS支持基于标准OAuth2协议,实现从IDaaS到业务应用的单点登录功能。

本文主要包含以下内容:

- 时序说明 OAuth2协议的简单时序图说明, 以及交互参数
- 主要流程 OAuth2.0模板使用主要流程
- 操作步骤 从新建开始配置一个OAuth2应用,以及如何在客户端中开发,包含具体API请求、响应和错误 提示
- FAQ 常见问题以及其对策

## 时序说明

#### 场景:SP发起单点登录时序

OAuth 2.0的草案是在2010年5月初在IETF发布的。OAuth 2.0是OAuth协议的下一版本,但不向后兼容 OAuth 1.0。 OAuth 2.0关注客户端开发者的简易性,同时为Web应用,PC应用和手机,和IOT设备提供专门 的认证流程。规范在IETF OAuth工作组的主导下,OAuth标准于2010年末完成。

OAuth2是一个授权协议, 主要用来作为API的保护, 我们称之为STS(安全令牌服务, Security Token Service)。但是在某些情况下, 也可以被用来实现WEB SSO单点登录。一般的流程是用户把发起页面的URL 和state参数关联上, 并保存在SP本地, 用户登录后, 可以获取一个Code, 利用Code拿到AT(Access Token)后, 可以利用这个AT获取用户信息userinfo,进而从state中, 获取到对应的原始URL,并跳转到这 个URL, 从而实现登录到一个业务应用SP的效果。本文档详细描述了这个SSO过程。

详细时序图(以授权码模式为例):



#### 说明:

#### 第[5]步参数要求

- response\_type:必选、值固定为"code"
- client\_id:必选、第三方应用的标识Ⅳ
- state:推荐、Client提供的一个字符串,服务器会原样返回给Client,它既能防止CSRF、XSRF, 同时也可以用来对应SP初始发起的状态。

- redirect\_uri:必选、授权成功后的重定向地址
- scope:可选、表示授权范围
- prompt:可选

#### 第[6]步校验内容

- a.client\_id是否合法
- b.prompt:
  - i. 若应用请求IDP时不带prompt参数,则逻辑为用户没登录就跳转到登录页
  - ii. 若应用请求IDP时带参数prompt=none,则默认用户已经登录验证,如果IDP发现用户未登录验证, 则直接报interaction\_required错误
  - iii. 若应用请求IDP时带参数prompt=login,则不论用户是否已经登录认证,都重新走一次认证流程

#### 第[11]步返回参数

• 跳转到[5]中指定redirect\_uri,并返回:code:授权码 state:步骤[5]中客户端提供的state参数原样返回

#### 第[13]步校验参数

● state是否和自己发送出的一致

#### 第[14]步请求参数

- grant\_type:必选、固定值"authorization\_code"
- code:必选、Authorization Response中响应的code
- redirect\_uri:必选、必须和Authorization Request中提供的redirect\_uri相同
- client\_id:必选、必须和AuthorizationRequest中提供的client\_id相同
- client secret: client的secret,用于授权服务器校验client的合法身份

#### 第[15]步校验参数

- a.client\_id、client\_secret(若有)是否合法
- b.redirect\_uri是否和步骤[A]中的redirect\_uri一致
- c.code是否合法:
- >是否过期
- >是否被重复使用,若是就视为一次攻击,加入日志审计,并将之前为code生成的access token撤销
- >比较code和应用的client id是否匹配
- d.server必须在http server头部返回: Cache-Control:no-store and Pragma:no-cache,确保client不会被 缓存

#### 第[16]步返回参数

- access\_token:访问令牌
- refresh\_token:刷新令牌
- expires in:过期时间

#### 第[19]步完成单点登录

 完成了这一步,就获取到access\_token和用户信息,可以展示当前登录用户信息,基于此保存的session 会话,用户可以不用再频繁登录,实现点击图标即可跳转应用的过程

## 主要流程

Step1 创建OAuth2应用,基于OAuth2模板快速创建应用 Step2 授权OAuth2应用,对OAuth2应用授予访问权限 Step3 获取应用信息,基于配置应用信息主要为获取授权码Code Step4 访问授权URL获取Code,通过相关应用配置,跳转应用地址 Step5 完成应用侧的开发/配置,就可以实现业务应用单点登录功能

### 操作步骤

Step1 创建OAuth2应用:

1、首先以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、点击左侧导航栏应用>添加应用选择右侧OAuth。



3、选择OAuth2应用模板点击添加应用。

添加应用 (OAu	th2)	$\times$
◎ OAuth2 应用只S	现了 SP(Server Provider, 业务系统方) 发起的单点登录流程。	
對标	<ul> <li>○ 上传文件</li> <li>図片大小不超过1MB</li> </ul>	
应用ID		
* 应用名称	OAuth2	
安全等级	5 请设置应用的安全等级,数字越大表示需要的安全等级越高,与认证源安全级别挂钩。	~
指定认证方式	跟随系统 当用户安全级别低于应用需求时,请用此处指定的方式进行强化认证。	~
* 应用类型	✓ Web应用 图移动应用 PC客户端 "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,如果想在多个环境中都显示应用则勾选多个。	,
* Redirect URI	请输入Redirect URI	1
	OAuth2 Redirect URI, 请以 http 或 https 开头。	~~
SP HomePageURL	请输入SP HomePageURL 应用首页地址,支持手动发起SSO。	
* GrantType	请选择 Authorization_Code: 授权码模式(即先登录获取Code,再获取Token),标准OAuth2流程; Implicit: 简化模式(在Redirect_uri的Hash传递 Token) 适用于验证第三方合法性时使用; PKCE:属于授权码模式的一个扩展,主要适用于无后端服务器来接收和处理Authorization Code按照 的应用。应用决定加密方式并生成密文,IDP通过校验密文的合法性来判断应用的身份,以此来增强应用满和IDP之间的校验,防止通信却持。	~ 双码
Access_Token有效期	7200 Access Token的运动时长(单位: 秒) 野认为7200(2/\时)	

4、Redirect URI:填写需要使用OAuth2单点登录应用的URL

GrantType : 选择authorization\_code

其他参数默认即可,有需要也可按照实际需要修改

#### Step2 OAuth2应用授权

应用授权:选择应用(搜索应用)、选择组织机构(搜索组织机构)、勾选授权即可

概范		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	^	<ul> <li>         应用接权     </li> <li>         管理员可以在这里使用不同方式为应用进行操权分配。     </li> <li>         IDaaS支持多件多样的接权方式:可以选定一个应用后,为其划定接权到的组织机构组的范围;也可以选定一个账户,并为其分配有权限访问的应用列表。     </li> </ul>
机构及组 账户管理 分类管理		应用 (1) 组织机构和组 (1) 已接权(1)个
认证 认证源 RADIUS 证书管理	^	1998/12013年2017年201
包 权限系统 应用授权	^	
审计	~	
其它管理	~	
2-34	~	

## Step3 获取应用信息

点击左侧导航栏应用>应用列表查看 OAuth2 应用详情,获得Client Id、Client Secret、Authorize URL.

概范		应用列表							应用分类
快速入门 ())用 ~ ())用列表		应用F 管理 当添加	時時後 意思可以在当時只愿管理已給活100分所有应用。应用可以实现 <b>单应管操和数据明</b> 终端力。 500两应用后,后点确认应用处于命用状态,并已给完成了接近,在应用冲描中,可以最到应用的评相信息,是点望是完地让,子和 <b>个能置</b> ,局炉能置,接近,审计编信息。						
用户目录 ^		<b>メ80時用</b> 際部入丘形合称 Q							
机构及组 账户管理		应用图标	应用名称	应用ID	应用分类		应用状态	二次认证状态	操作
分與管理		J	JWT1126	contract the					授权 详情 ▼
认证 へ 认证源		J	JWT1120						授权 详情 ▼
RADIUS 证书管理		<b>O</b> ALTH	OAuth2题试	2220/224222	统计分类				授权 详情 🔺
授权 个									
权限系统 应用授权		应用信息		账户信息 - 同步		账户信息 - 子账户		授权信息	
★	,	应用的详细信息		SCIM协议设置以及把组织机构、组同步推送至应用		平台主账户与应用系统中子账户的关联系	R.	应用与人员组织的授权关系	
其它管理	,	室翻洋橋	修改应用 删除应用	同步机构 SCIM配置		查看应用子账户		授权	
设置		审计信息		API		管理应用内权限			
		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			
		查看日志	查看同步记录	API Key API Secret		御定权限系统			
		sts	JWT STS(附网关保护)1111	wangliplugin_jwt_sts1	统计分类				授权 洋情 ▼

应用详情 (OAuth2测试)

图标	OAUTH
应用ID	10.02 (5-402 (2
应用名称	OAuth2测试
应用Uuid	<ul> <li>All Scholar SCOVET CONTRACTOR CONTRACTOR CONTRACTOR</li> </ul>
安全等级	5 ~ 请设置应用的安全等级,数字越大表示需要的安全等级越高,与认证源安全级别挂钩。
指定认证方式	题随系统 当用户安全级别低于应用需求时,请用此处指定的方式进行强化认证。
应用安全等级	无
Client Id	
Client Secret	
Redirect URI	
SP HomePageURL	
GrantType	authorization_code
Authorize URL	https://www.migrim.wimmanager.com/oauth/authorize? response_type=code&scope=read&client_id=????????????????????????????????????

Step4 登录获取Code

参考SP发起单点登录时序:认证成功生成code

应用通过一个IDP登录按钮等或其它方式, 触发浏览器打开 AuthorizeURL, 使用**授权的账户**进行登录, 登录 成功后跳转到回调地址redirect\_uri, 并把Code参数一同转发过去。
			X	
	简体中文	扫码登录更便捷	34	
		D		
		IDP		
0	- +			
		忘记密码		
		提交		t
		方认证登录	-	
Ā		em 🛐		

### Step5 完成应用侧的开发/配置

5.1、利用Code从服务器获取AT(Access Token)

参考SP发起单点登录时序:请求access\_token

无论是JAVA, PHP, 还是.NET应用, 接下来要做的是,应用通过URL参数拿到这个Code 后, 紧接着构建一个应用Token 换AT(Access Token)的过程。

Request URI: https://{IDaaS\_server}/oauth/token?grant\_type=authorization\_code&code= {code}&client\_id={client\_id}&client\_secret={client\_secret}&redirect\_uri={redirect\_uri}

IDaaS\_server:为实例用户登录页地址(推荐使用)、实例开放接口域名也可以使用

应用身份管理	实例列表							
概览页								
EIAM 实例列表	实例ID/名称	标准版实例ID	状态 (全部) 🗸	规格授权	最大用户数	到期时间	产品版本	用户登录页地址
CIAM 实例列表	idaas-cn-hangzhou-kt-?j0.0 and 1	idaas-cn-09x tour 1000	运行中	增强版	100	2021年1月2日	V1.7.7	q <b>ətriyidə</b> login aliyunidaas.com
产品文档								
联系我们								

注: OAuth支持多种grant\_type 这里使用的是authorization\_code模式。

接口说明:获得 access\_token

### 请求方式:POST

请求参数

### 单点登录配置·标准协议模板使用指南

参数	类型	是否必选	示例值	描述
code	String	是	vuQ3n6	用户登录成功后回 调传递的code值
client_id	String	是	oauth2 client_id	OAuth2 client_id
client_secret	String	是	oauth2 client_secret	OAuth2 client_secret
redirect_uri	String	是	http://example.c om	重定向 url

○ 返回参数示例:

```
{
    "access_token": "b833ca9f-82f7-485e-a18a-4e3e2422f808",
    "token_type": "bearer",
    "refresh_token": "073283f5-6263-4130-86bd-64cbafbaae94",
    "expires_in": 7199,
    "scope": "read"
}
```

参数	类型	示例值	描述
access_token	String	333ab704-abc0-48b3- 8af0-496eedd15383	Access Token
token_type	String	bearer	Token 类型
refresh_token	String	073283f5-6263-4130- 86bd-64cbafbaae94	刷新token
expires_in	String	7199	Access Token 过期时间
scope	String	read	申请的权限范围

• 错误码说明

HttpCode	错误码	错误信息	描述
400	invalid_grant	Invalid authorization code: "code".	无效的授权码
400	invalid_grant	Redirect URI mismatch.	重定向 URI 不匹配
401	Unauthorized	Unauthorized	未授权的访问
403	Forbidden	Forbidden	无权限访问
404	ResourceNotFound	ResourceNotFound	访问的资源不存在
415	UnsupportedMediaTyp e	UnsupportedMediaTyp e	不支持的媒体类型
500	InternalError	The request processing has failed due to some unknown error, exception or failure.	发生未知错误

① {code}需要替换为授权应答Authorization Response中提取到的 code 参数的值。

注意 Code 的值只能用一次

②{client\_id}、{client\_secret}需要替换为认证成功生成code中获得的值

③ {redirect\_uri} 需要替换为302重定向到IDP进行认证授权添加 OAuth2 应用时输入的跳转值

以上完成后你将获得AT(Access Token),此AT将作为你访问的凭证。

### 5.2、获取用户信息userinfo

参考SP发起单点登录时序:应用请求userinfo(携带access\_token)

在获取到AT(Access Token)后,应用可以接着向IDaaS平台发送进一步的请求,以获取到用户信息,实现 登录到一个业务应用SP的效果。

①发送GET请求到https://{IDaaS\_server}/api/bff/v1.2/oauth2/userinfo?access\_token={access\_token}

{access\_token} 替换为前一步获取到的AT(Access Token)

②从返回参数即可获取userinfo信息

Request URI: https://{IDaaS\_server}/api/bff/v1.2/oauth2/userinfo

- 接口说明:获取用户详细信息
- 请求方式:GET
- 请求参数

参数	类型	是否必选	示例值	描述
access_token	String	是	333ab704-abc0- 48b3-8af0- 496eedd15383	Access Tok

### ■ 返回参数响应示例

```
{
    "success": true,
    "code": "200",
    "message": null,
    "requestId": "149DA248-8F49-4820-B87A-5EA36D932354",
    "data": {
        "sub": "823071756087671783",
        "ou_id": "2079225187122667069",
        "nickname": "test",
        "phone_number": 11136618971,
        "ou_name": "阿里云IDAAS",
        "email": "test@test.com",
        "username": "test"
    }
}
```

```
}
```

### ■ 参数说明

参数	类型	示例值	描述
success	boolean	true	是否成功
code	String	200	状态码
message	String	null	返回消息
requestId	String	B3776BB1-930F-4581- B4C3-18F2D7D136CA	请求ID
data	Object	响应数据	
sub	String	823071756087671783	子编号
ouid	String	2079225187122667069	父组织ID

参数	类型	示例值	描述
nickname	String	test	昵称
phone_number	String	11136618971	手机号
ou_name	String	阿里云IDAAS	父组织名称
email	String	test@test.com	邮箱
username	String	test	用户名

■ 错误码说明

HttpCode	错误码	错误信息	描述
401	Unauthorized	Unauthorized	未授权的访问
403	Forbidden	Forbidden	无权限访问
404	ResourceNotFound	ResourceNotFound	访问的资源不存在
415	UnsupportedMediaTy pe	UnsupportedMediaT y pe	不支持的媒体类型
500	InternalError	The request processing has failed due to some unknown error, exception or failure.	发生未知错误

这样,用户登录成功后,浏览器有了主会话,一个SP应用利用它获取一个令牌 AT(AccessToken),应用拿到AT令牌后去IDaaS认证中心校验令牌是否有效,同时到/userinfo接 口去拉取更多的用户信息,获取到具体的子账户Userld,有了Userld就可以创建SP的子会话。从而 在子会话有效期都不用再登录,实现从IDaaS单点登录到应用的全过程。

### FAQ

1. 如何强制用户登录认证?

在登录接口增加prompt参数,当prompt=login则强制跳转登录页,也就是在下图 Authorize URL后面 增加"&prompt=login"则不论用户是否已经登录认证,都会展示登录页,用户必须进行一次认证,才可 继续单点登录流程。

https://cjl.idaas.test.com/oauth/authorize?response\_type=code&scope=read&client\_id=825d9cffb88a e45d023ae08cd5eb4ca6yk5YBPePbqV&redirect\_uri=http%3A%2F%2Flocalhost%3A8082%2Fasd&state =38e78b11072df978a89138144e6e0933zxm3GeFnjLi\_idp&prompt=login

2. 如何保存初始发起页面?

在SP发起一个SSO请求的时候, SP需要能够把对应的URL, 保存在内存中, 并和OAuth中的State参数关联起来。这样, 在IDaaS返回State后, 可以找到当初的URL, 并跳转到这个URL, 实现 DeepLinking。比如使用了JAVA的Spring框架的话, 可以用SavedRequest来完成。

## 2.4. C/S(程序)模板使用指南

唤醒程序后通过OIDC协议向其传递参数实现登录,适用于可以接收解析OIDC协议参数的应用。

#### 操作步骤

1. 在左侧导航栏, 点击**应用 > 添加应用**, 选择C/S程序应用模板, 点击**添加应用**。

```
添加应用 (C/S程序)
```

♀ C/S应用单;	点登录需要先安装 IDP-Agent程序
应用图标	
	◎上传文件
	图片大小不超过1MB
* 应用名称	C/S程序
* 可执行文件	如: abc.exe
	C/S应用启动的可执行文件
可执行文件路径	如: C:\User\AppData\abc\
	可执行文件路径
传递参数	如: d=idp&m=code
	在打开C/S应用程序时传递的固定参数
*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
? 说明	C/S应用如果要完成单点登录,需要本地安装IDP-Agent插件。
◦ 应用名称:	根据实际情况进行填写,为必填项;
+	
ㅇ 미 /시/ㅜ乂1	4. 盖安埠与1/212用后刘州执行又件名称

- 可执行文件的路径: C/S应用文件在本地计算机的位置
- 2. 开启应用并授权,默认是按应用授权组进行授权。

请输入应用名	称	٩			
应用图标	应用名称	应用ID	设备类型	应用状态	操作
Ē	C/S程序	idaas-cn-v6417ukc30ecs_oldc2	PC客户踌		援权 详情 ▼
J	JWT345	idaas-cn-v6417ukc30ejwt13	Web应用		授权 详情 ◄
J	DefaultAppfor自己测试connector	ab2ea53c87a0796c4dc2836fe57f3250Bhjn4BX6aVz	数据同步		授权 详情 ▼
J	DefaultAppfor58正式	35a03ddef477f8082c81fdca2898235aO6B2yHNCIXY	数据同步		授权 详情 -
C-)	RAM	idaas-cn-v6417ukc30eallyun5	Web应用		授权 详情 ▼
J	S	idaas-cn-v6417ukc30ejwt12	Web应用		授权 详情 ▼
C-)	阿里云 用户 SSOzb100	idaas-cn-v6417ukc30eallyun4	Web应用		授权 详情 ▼
OMETH	OAuth2	idaas-cn-v6417ukc30eoauth23	Web应用		授权 详情 ▼
<b>C</b> -J	阿聖云 用户 SSO(scim)	idaas-cn-v6417ukc30eallyun3	Web应用		授权 详情 ▼
salesforce	Salesforce	idaas-cn-v6417ukc30esalesforce	Web应用		授权 详情 ▼
应用授权	148 医肉球肌肉带 医蛋白球肉肉 医肉带球肌蛋白			共51条 〈 1 2 3 ***	6 → 10 余页 ~ 就至 1 页
按应用授助					
♀ 管 □□ 应用 (3)	理员可以在这種使用不同方式为应用进行硬份分配。 aa8 支持多件多样的授权方式:可以透定一个应用后,为其划定批	积到的组织机构组的范围;也可以选定一个账户,并为其分配有 组(86)已颁权(0)个	权限访问的应用列表。		
C/S程序		📄 : 代表组织机构, 💩 : 代表组。			
C/S程序	:	请输入组名进行搜索			
C/S程序	測試	□ □ ● 阿里云IDAAS			
C/S程序	大3条 《 1				

- 3. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
- 4. 在用户首页点击C/S应用图标

我的应用					
Web应用					
<b>に</b> 阿里云 角色 SSO2b100 米気切除户	WordPress-SAML-勿删 米品切醉户	CAS(Kott)	CIS程序	jwt demo #:@sz@#:P	<b>て</b> の理云 用户 SSO 米統部件
<b>C-D</b> 顾田三 你会 \$50	同日前第一次期	<b>[-]</b> 阿里三 你会 SSOLD	<b>[-]</b> 阿里王 田白 550 勿樂	FORM	
東京加紫色	中国王和中国"201033 朱添加派户	中国主义 用已 530-55	◎ <u></u>	-2011(9月7日) 来添加账户	永远间 ( )项 ( ) 来派加张卢
J	salesforce	W	SAML		
JWT-勿删	Salesforce 未添加账户	WordPress-SAML-917 未添加账户	SAML-勿删 未添加账户		

根据页面提示,添加应用的子账户

您尚未添加该应	7用的账户关联,请先关联后才能使用.	
提示:此应用采用的是寻 关联(你能看到此提示:	=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; 表明后台尚无关联纪录) 。	或是管理员直接为你设计
子账户*	子账户	
	即您在此应用中的账户	
	得获账户关键	

添加完子账户以后,在用户页面可以点击C/S图标进行单点登录。

# 2.5. 表单代填模板使用指南

本文为您介绍IDaaS通过表单代填,实现应用的单点登录的功能。

## 背景信息

假设公司将某应用A作为企业的网站,日常访问频繁。传统的访问方式便捷性差且存在安全隐患。

- 应用A日常办公使用频次高,登录繁琐且耗时长;
- 应用A登录未通过验证码进行身份鉴别,存在安全隐患;

### 解决方案

通过应用身份服务的应用管控(Application)功能,使用其中的表单代填应用模板实现对A应用的单点登录 以及身份的鉴别。

### 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. 在左侧导航栏,单击应用>添加应用,选择表单代填应用模板点击添加应用

欢迎·IDaaS	添加应用					
~ 控制台	<u>- 25</u> 53	治议 定制構板				
概范						
快速入门	表单			٩		
审批中心	the second	0000	1-10		VLAT NE BU	19.0-
~ 应用	WEHH BEINK	82/H3 C449	10.00	reach	拉爾內里	SKTF
应用列表	F	表单代填	SSO, AES256	思拳代動可以機抑用中容量更加輸入用户各和底局,再通过患拳描点的一种量更方式。应用的原母底带在 IDaaS 中使用 AES256 IDaaS并在地的密存储。很多旧有高统,不支持标准认证协议的 系统成不支持政策的系统可以使用患拳代面实现他一番份管理。患单中有图片验证码、CSRF token、现态参数的场级不适用。	WEB	添加应用
794042275						
∧ 用户				共19	K 1 3	創至 1 页
账户及组						
账户管理						
~ 摂权						
应用授权						

3. 在添加应用对话框中,填写应用的信息

添加应用(表单代填	ũ)
应用图标	FORM ⊕上传文件 图片大小不趨过1MB
* 应用名称	表单代填
* 所属领域	私有云
* 设备类型	✓ Web应用
登录 URL	http://
	AES256登录界面的访问地址,以http://或https://开头,如:https://oa.xxxx.com/login;若登录页面是移动端,则勾选上"移动端"
* 登录提交 URL	http:// AES256登录表单提交的完整URL,以http://成https://开头,如: https://oa.xxxx.com/signin
* 登录名属性名称	usernameField
	username标签的name属性
* 登录密码属性名称	passwordField
登寻检纽居州夕教	berrand in the second s
	Subminined 登录按钮标签的name属性
登录其他信息	登录其他信息
	登录时表单中需要的其他一些信息,若有则填写, 如: <input name="spt" type="hidden" value="123"/>
登录成功跳转地址	loginSuccessPage
	登录成功后期转地址
* 登录提交方式	● POST ○ GET
* 账户关联方式	○账户+密码(系统按主子账户对应关系手动关联应用的子账户和密码)
	提交 取消

- 提交登录URL: 应用A的登录接口
- 登录名属性名称:登录接口的登录名
- 参数登录密码属性名称:登录接口的登录密码
- 。 参数登录提交方式:登录接口的请求方式
- 。 账户关联方式: 账户和密码
- 4. 启用应用并授权

= (-)阿里云		Q. 1928		調用	I# ## 22 336688 [] () [] #
< 1000	前用列表				
85	<u>所有的成</u> 私有云 公有云 移动 物部用 同能控制 网络				
へ 政用 ①用刊表	1840人出现2010 1		<b>Q</b>		
深城应用	应用器标 应用名称	8780	设备关型	应用状态	目的
》 1804 陈卢及后	Final States	idaas-cn-mpil15hd7v0faas256	2058		· 授权 · 评值 •
死の管理					
へ <b>滅収</b> 応用地収	a Pista	LEGR	類の供意 - 子強の相子のU	<b>月</b> 章 技能推用	
和限制的	应用的评估信息(如用近可编唱)	应用的单合重要地站	平台主OU版户对应应用系统中于OU版户的关联表	应用与人员临时的时间	见光虹
∧ iAIE	或者IPF信 经改正用 数96应用	ID and SEETING	最重应用 <b>学</b> 家/*	1967.	
い正規 征引管理	用计信息	API			
Radius					
へ 単計 委作日志	重要回用系统年间的操作日本。 编码因为文全 重要日本 查要用少记录	应用的外周用的API的口 API Key API Secret			

= (-)阿里云		Q 腔索
← 返回	应用授权	
首页	按应用接权组 按组接权应用	
^ 应用		
应用列表	应用 (1)	<b>组 (2)</b> 已授权 (0个)
添加应用		
∧ 用户	<b></b> 表单代谊	提示:授权时,子级组会默认继承父级组的权限,若要单独取消子级组权限,请解除父子级组之间的关系即可。
账户及组	表单代填 >	请输入组名进行搜索
账户管理		□-□
∧ 授权	共1条 < <mark>1</mark> >	
应用授权		是否向下演历 (演历被洗中的组的下级组, 端删应用的权限)
权限系统		此操作將批量改变账户及组的授权,可能耗时软长,将影响用户所能访问的应用
~ 认证		保存
31.3正语		

5. 绑定主子账户。其中主账户是IDaaS平台的账户,子账户是应用A中的账户

	Web -	所有领域 私有云 公有云 移动	物联网 网络控制	其他					
AkJ       j	ERE .								
NATURAL	(道入门) [1	表单			٩				
Image: micic       verweichtigt       MEM       ME	10++0	应用图标 应用名称		应用ID	设备类型		应用状态	次认证状态	操作
	2用列表	<b>下</b> 表单代填		wceshiaes25618	浏览器				授权 洋情 ▼
A         Mark (MAR)	Abu应用	FORM							
	5	<b>下</b> 表单代值0527		wceshiaes25617	浏览器			×	授权 详情 🔺
Notes         Notes         Notes         Notes         Notes           Rate         <	户及组 (由*****								
	7	应用信息		认证信息		账户信息 - 子账户	同步	授权信息	
RBR     RBR     DAXBERS     RBR     RBR     RBR     RBR     RBR       RBR     RBR     RBR     RBR     RBR     RBR       RBR     RBR     RBR     RBR     RBR     RBR       RBR     RBR     RBR     RBR     RBR     RBR     RBR       RBR     RBR     RBR     RBR     RBR     RBR     RBR     RBR       RBR	、 (用授权	应用的详细信息 (使用后可编辑)		应用的单点登录地址		平台本OU账户对应应用系统中于OU账户的	关联表	应用与人员组织的接权关系	
	現系统	查看洋街		IDaaS发起地址		查看应用子账户		授权	
winder       An         winder       winderse         winderse	E								
alse statustication and and all the a	1注版 E书管理	审计信息		API					
••••••••         ••••••         ••••••         ••••••         ••••         ••••••         ••••••         ••••••••       ••••••••••        •••••••• </td <td>adius</td> <td>查看应用系统详细的操作日志,确保应用安全</td> <td></td> <td>应用对外调用的API接口</td> <td></td> <td></td> <td></td> <td></td> <td></td>	adius	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					
Attribute	+	查看日志 查看同步记录		API Key API Secret					
主称・低い合い       マロ・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー・ロー	← 子账户 <sub>表单代填0527</sub>							深加明户关注	批型导入 批
主政合         予数分         記込券         予数分         記載分         記載公         注意知         注意	主账户 (账户名)			٩					
Tett53         dmm         Tett53         Adm         Tett53         Adm         Tett53         Adm         College         Colege </th <th>主账户</th> <th>子账户</th> <th>显示名称</th> <th>子账户密码</th> <th>是否关联</th> <th>审批状态</th> <th>关联时间</th> <th>)</th> <th>操作</th>	主账户	子账户	显示名称	子账户密码	是否关联	审批状态	关联时间	)	操作
133035401       Admin       133054001       조       단規       조       2019-05-20	Test183	admin	Test183	无	已关联	无	2019-05	-29	制种
draven draven draven 중 표 단規 표 2019-05-27 2019-07 2019-05-27 200-00-00-00-00-00-00-00-00-00-00-00-00-	18380581401	admin	18380581401	无	已关联	无	2019-05	-29	##+
共3条 〈 1 〉 厳至 1	draven	draven	draven6	无	已关联	无	2019-05	-27	激除
								共3条 <	1 > 跳至 1

## 6. 登录已授权该应用的普通用户, 点击图标进行单点登录

欢迎 · IDaaS	我的应用
	免登应用
首页	
应用管理	
应用子账户	F
设直 ^	гоки
我的账户	AES256表单代填(测)
二次认证	
我的消息	
我的日志	仅支持移动端免登应用
	尚未获取到移动端免登应用。

若以上步骤全部成功完成,即可实现使用表单代填单点到应用A。

## FAQ

### 1. http应用是否可以使用表单代填

不可以。IDaaS是https请求, SP是http,从https往http请求会被浏览器的安全机制给限制,需要SP支持 https才行。

### 2. 前后端分离的应用是否支持表单代填

不支持。有图片验证码 或者 前后端分离的应用不支持表单代填。

### 3. 如何获取登录的请求连接和登录参数

在SP登录页面,通过F12打开network,获取到登录请求的url。

	<b>)</b> 山	登录到。 <mark>第</mark> 款UA				
	请输入账户					-
	请输入密码					
	我的政权	登录 2000年				
🕞 Elements Console Sources Network Performance Memory Application Security Audits						
● ◎   ▼ ♀						
Filter Hide data UKLS MI XHR JS CSS Img Media Font Doc WS Manifest Other Only show n	200 ms 220 ms 240 ms	260 ms 280 ms 300 ms	320 ms 340 ms	360 ms 380 ms	400 ms 420 m	s 440 mi
Name × Headers Preview Response Initiator Timing Cookies						
signin 1 v General						
login?authentication_error=1 Request URL https://j+1.6/prov.oc						
bootstrap.min.css Request Method: POST						
Status Code: 9 302 Found						
Remote Address: 47.108.98.284.000						

并且获取到登录的参数,添加到IDaaS的表单代填模板中。

### 单点登录配置·标准协议模板使用指南

20 ms 40 ms		60	60 ms 80 r		100 ms	120 ms		140 ms		
Name		×	Headers	Preview	Response	Initiator	Timing	Cooki		
signin		3	Sec-Fetcn-Wode: navigate							
login?auther	ntication_error	r=1	Sec-Fetch-Site: same-origin							
bootstrap.mi	in.css	5	Sec-Fetch-User: ?1							
<ul> <li>loginba.png</li> </ul>			Upgrade-Insecure-Requests: 1							
<u>99</u>		User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)								
Form Data view source view URL encoded      username: 123      nassword: 123										
4 requests 3	80 KB transfe	rred 🗌	/assw010.	125						

添加应用(表单代)	直)
图标	<ul> <li>         ・ ・ 上传文件         </li> <li>         图片大小不超过1MB     </li> </ul>
* 应用名称	表单代填
* 应用类型	✔ Web应用 "Web应用"只会在用户Web使用环境中显示。
* 登录 URL	http:// AES256登录界面的访问地址,以http://或https://开头,如:https://oa.xxxx.com/login;若登录页面是移动端,则勾选上'移动端'。
移动端	
* 登录提交 URL	https://xxxx.signin AES256登录表单提交的完整URL, 以http://或https://开头,如:https://oa.xxxx.com/signin
* 登录名属性名称	username Username标签的name属性
* 登录密码属性名称	password Password标符的name属性
登录按钮属性名称	submitField 登录按钮标签的name属性
登录其他信息	登录其他信息
	登录时表单中需要的其他信息,若有则填写,如: <input name="spt" type="hidden" value="123"/>
* 登录成功跳转地址	登录成功跳转地址
	登录成功跳转地址
* 登录提交方式	● POST ◯ GET
* 账户关联方式	○ 账户+密码 (系统按主子账户对应关系手动关联应用的子账户和密码)
	<b>提交</b> 取消

### 4. 应用不支持表单代填,如何进行单点登录对接

如果是支持标准协议的,可以使用SAML等协议对接;如果是自建应用,支持改造的,可以使用JWT进行单 <mark>点登录</mark>,或者使用OAuth2方式对接,IDaaS建议使用JWT方式对接。

# 3.主子账户介绍

本文介绍如何通过应用管理功能添加应用子账户。通过添加应用子账户,用户可以通过IDaaS单点登录到其他应用。

## 背景信息

传统应用的登录方式通过输入用户名和密码,随着日常办公软件数量的不断增加、用户需要记忆多套用户名和密码,给用户带来负担;统一所有用户名和密码固然方便,却会令企业账户体系面临严重的安全隐患。

### 解决方案

IDaas提供单点登录功能,只需使用单点登录协议和应用对接,并完成主子账户的绑定,即可实现一次登录 访问所有授权应用的目的。应用之间后续进行切换时,无需再次输入用户名和密码,全面提升用户办公效 率。

## 主子账户介绍

在进行单点登录时, IDaaS 会向应用系统传递对应的子账户, 该子账户需要在应用系统中存在且可识别。

主账户: 主账户指的是 IDaaS 中的账户;

子账户:子账户指的是在指定应用系统中,用户会以什么身份进行访问,是单点登录时带给应用的身份标识,存在于对接的第三方业务系统中。

示例:

在IDaas的机构及组中创建了gc\_test这个账户,该账户在绑定主子账户的时候是作为主账户存在。

一	组 组织机构						
新建账户	账户名称 >	请输入账户名称进行搜索	Q	搜索			
当前账户数 2	25 / 已购套餐规格为 \$	500					
编号	账户名称	显示名称	类	型目示	ł	操作	
1	gc_test	gc_test	自	建账户 /		修改转岗账户同步	同步记录 离职

在对接的第三方业务系统中,存在gc\_zzh这个账户,该账户在绑定主子账户时是作为子账户存在。

欢迎来到 JWT								admin iB
★首页	Type username	Q 共: 226 个用户						• (1)
▲ 应用	Ho?	100	- C.	权限	创建时间	用户类型	同步结果	Pik
<b>1</b> 用户	gc_zzh 🖯	迷户	58@qq.com	[USER_ACCOUNT]	2021-06-25 03:55	系统创建	同步成功	无
主約	0		abc.com	[USER_ACCOUNT]	2021-06-02 02:25	SCIM同步	无	/ 阿里:
1 10/01010	in 🛛			[USER_ACCOUNT]	2021-06-01 06:14	SCIM同步	无	// 升降的
▲ 组织积48	n ng 🛛			[USER_ACCOUNT]	2021-06-01 06:14	SCIM同步	无	// 升降级
<b>三</b> 消息	a			[USER_ACCOUNT]	2021-05-28 08:05	SCIM同步	无	// 升降级)
◆ 系统设置	x		> om.cn	[USER_ACCOUNT]	2021-05-28 07:54	SCIM同步	无	// 升降级8
* SSO	2 g <b>O</b>		zhu. "ing@com.cn	[USER_ACCOUNT]	2021-05-28 07:40	SCIM同步	无	// 升降级浪
	2	1		[USER_ACCOUNT]	2021-05-28 07:38	SCIM同步	无	/ 阿里云ID/
		111		[USER_ACCOUNT]	2021-05-28 07:38	SCIM同步	无	/ 阿里云IDA
				[USER_ACCOUNT]	2021-05-28 07:38	SCIM同步	无	/ 阿里云IDA
								« 1 2 3 4 5

从应用管理页面,点击查看应用子账户,可以进行主子账户绑定。

添加账户关联		$\times$
	Г	
* 主账户	gc_test	
* 子账户	gc_zzh	
	保存返回	

该主子账户绑定后,以gc\_test这个账户登录IDaas用户端,点击对应的应用进行单点登录,IDaaS 会向应用 系统传递对应的子账户gc\_zzh,最终以gc\_zzh的身份登录到第三方业务系统。

aS统一认证身份平台					消息	gc_test + 📋 切换语言 ·
! · IDaaS	我的应用 搜索应用	٩				
	Web应用					
应用管理 应用子账户 <b>设置 ^</b> 我的账户 二次认证	<b>C-D</b> 阿佃云RAM·用户SSO	SAML-555	CAS((838), Jenkins	OAUTH OAuth2	<b>の</b> の <sup>支持で道</sup> 未満2009/ <sup>10</sup>	OAuth2-baldu
的消息的日志		<b>C-D</b> 阿显云RAM.角色SSO 末該加熱户	AO	J <sub>WT</sub>	GitLab SAML_Gitlab	OAuth2-grafana
	移动应用					
	CAS((5)E)-Jenkins	J <sub>WT</sub> JWT	OAuth2-grafana			
k.login.aliyunidaas.com/a	pi/bff//go_c0406983e60d4b9827df64fffa6	f73f282l3WHcbICG				
迎来到 JWT						gc
首页 应用 用户	登录到	第三方应用				
组织机构 消息 SSO	<ul> <li>登录信息</li> <li>用户名 gc</li> <li>登录次数 1</li> </ul>	zzh				
	2021					
	SC	Thereare				
	SCIM					
	100 Bar					

账户关联方式介绍

管理员在添加应用的时候,可以选择账户关联的方式,账户关联方式分为两种:账户关联和账户映射。

- 账户关联:系统按照子账户对应关系进行手动关联,适合主账户和子账户名称不同的情况;
- 账户映射: 指系统自动将主账户名称作为应用的子账户, 适合主账户和子账户名称相同的情况。

☰ (-)阿里云	命 工作台			2%
概応	应用列表		修改应用 (JWT	n ×
应用 ^ 应用列表	<ul> <li> <u>应用列表</u>          餐理员可以在当前页面管理已经质加的所有应用,应用可 出添加均应用后,应该确认应用处于应用状态,并已经知      </li> </ul>	以实现 <b>单点登录和数据同步</b> 能力。 成了授权。在应用详细中,可以看到应用的详细信息。	target_url	中心哲学活動活動化物は、加二http://www.xxx.com/service/message 中心哲学成功后、会在 DaaS 跳转号 redirect_url 對和は_loken同时情景,一般用于能转号deeplinking的一级菜中、指定页面等,此项可选。
294/402/HB 账户 ^	海仙成用。清榆入应用名称		SSO Binding	REDIRECT ~ 单应控录库方式,REDIRECT为GET类型
009000 账户管理 公告管理	应用跟标 应用名称 *	应用iD	ID_Token有效明	600 ID_Token的行动规则,单位29: 69
以证 ~ 认证	く <u></u>  4998	idaas-cn-0ju251c9l01plugin_aes256	是否显示应用	変更 限収給用や后, 豊香在用や首次園示,
RADIUS 证书管理	JMT JMT		是否脱敏参数	医五极的dToken中的于机号、邮箱参数
授权 へ 权限系统	应用信息 	<b>认证信息</b>	SP支持退出	乙酸用皮防退出,请勾施上并填写SP退出地址:
应用授权 审计 ~	而HHEDHHHMIAG	itDaaS发起地址 SP发起地址	SP退出地址	http://182.92.68.138.6400/jw/180-09160550433872053431/ng_logout 应用操作社IPP專用指引属出地址: 当全局属出想引,会阐用此地址通出此点用
其它管理 ~ · · · · · · · · · · · · · · · · · ·	授权信息	审计信息	* 账户关联方式	● 数件关键(係税检注子数/中均应关系进行手动关键,用户语加后需要管理员申询) ● 数件地数(係税自动用主数件名称或加定的分段处约为应用的子報/中)
		查看应用系统详细的操作日志 查看日志 查看同步记录	L	<b>御文</b> 取消

当选择账户映射时,如下图登录IDaaS门户后,不需要手动给用户关联子账户,会自动根据主账户生成同名的子账户,并自动进行主子账户绑定。

IDaaS统一认证身份平台					消息	gc_test ▼ 📋 切换语言 ∨
欢迎 · IDaaS	我的应用 搜索应用	٩				
主导航 ^	Weber					
首页	NEDETH					
应用管理						
应用子账户	<b>[</b> -]	S	C		On	
设置 ^		SAML	CAS	ОЛИТН		OAUTH
我的账户	阿里云RAM-用户SSO	SAML-sss	CAS(标准)-jenkins	OAuth2	表单代填 <b>未添加账户</b>	OAuth2-baidu
二次认证						
我的消息	æ					
我的日志	( ALA )	[-]	OA	J	👐 GitLab	Ο
	电和器制 本的代语 just	展用元RAM、负伯SSO	JWT	JWT	SAML Gittab	OAuth2-grafana
	未添加账户	未添加账户				on an a-granana
	移动应用					
	CAS	TWL	OAUTH			
	CAS(标게)-jenkins	JWT	OAuth2-grafana			

账户关联的方式,如何进行绑定主子账户请查看手动绑定主子账户。

## 应用授权

创建好应用后,需要确认应用是开启状态,并点击授权,将应用授权到IDaaS账户或者组织机构。

概览								
快速入门 应用 ^	应用列表 管理员可以在当前页面管理 当添加完应用后,应该确认	已经添加的所有应用,应用可以实现 <b>单</b> 应用处于启用状态,并已经完成了授权	<b>点登录和数据同步</b> 能力。 。在应用详情中,可以看到应用的详细作	. <b>忠、单点登录地址、</b> 于	子账户配置、同步配置、授	权、审计等信息。		
添加应用	<b>添加应用</b> 请输入应用名称			٩				
账户 ^ 机构及组	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
账户管理 分类管理	表单代填_jwt	ida	as-cn-0ju251c9i01plugin_aes256	Web应用				授权 详情 ▼
认证 ^ 认证源	JWT AO	ida	as-cn-0ju251c9i01plugin_jwt	Web应用				授权 详情 🔺
RADIUS 证书管理	应用信息	ы	正信息		账户信息 - 同步		账户信息 - 子账户	
授权 へ	应用的详细信息	181	用的单点登录地址		SCIM协议设置以及把组	织机构、组同步推送至应用	平台主账户与应用系统	的关联表
权限系统 应用授权	<b>查看详情</b> 修改应用 删	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	aaS发起地址  SP发起地址		同步机构 SCIM	511	查看应用子账户	
<ul> <li>审计 ~</li> <li>其它管理 ~</li> </ul>	授权信息	审计	十值息		API		管理应用内权限	
设置 、	应用与人员组织的授权关系	查	香应用系统详细的操作日志		是否对应用开放系统AP	I	管理应用内菜单与功能	級权限
	授权	查	看日志 查看同步记录		API Key API Sech	tt IP 白名单配置	绑定权限系统	
	回里云 命 工作台							Q
概览	应用授权	z						
快速入门	应用授权	主体 主体授权应	用					
应用	^							
应用列表	ф. <b>П</b>				副作	49 494 <b>∩</b> ±0±∕		
添加应用		_			火以一	组 组织你的	3 刀矢	
账户	JWT			Q	请输入账户名	称进行查找		
机构及组	JWT	-		>	☑ 自身赋予	的权限资源 🛛 돈	色自身赋予的权限资	题 🔽 继承 (组、)
账户管理	表单件	這 iwt		<u>```</u>				
分类管理						长户名称		
认证	^ JWT			>	✓ g	c_test		
认证源 RADIUS			共3条 〈	1 >	У	NOP		
证书管理								
授权	~					In the second		
权限系统					n	ing sugrenu		
应用授权					6	- 400		

## 手动绑定主子账户

手动关联子账户可以分为两种方式:

- 由管理员直接操作。
- 由用户本人进行申请,管理员对用户的申请进行审批
- 1. 由管理员直接操作

### 1.1 手动1对1绑定

管理员点击应用的"详情"按钮,点击"查看应用子账户"即可对应用的所用子账户进管理,包括添加应用 子账户操作。

	里云	★ 工作台				Q 搜索	费用	工单	备案	企业 支持	App	E (	}, ≞	⑦ 简体	: (
概览 快速入门		应用图标	应用名称	应用ID	设备类型		应用状态		二次认证状	ō			操作		
应用 <b>应用列表</b>	^	(44) 2 - (5) 3 - (5) 3 - (5)	1000		Web应用				×			授权	洋情 ▼		
添加应用	^	OA	JWT	Jwt	Web应用				×			授权	详情 🔺		
机构及组 账户管理		应用信息		认证信息		账户信息 - 同步			账户(	言息・子账户					
分类管理 认证	^	应用的详细 查看详情	<b>新信息</b> 修改应用 删除应用	应用的单点登录地址 IDaaS发起地址 SP发起地址		SCIM协议设置以及把组织机构	勾、组同步推送至应用		平台: 查看)	<del>上账户与应用</del> 应用子账户	<del>7640-1-79</del>	中的关系	祛		
认证源 RADIUS 证书管理		授权信息		审计信息		API	~	D	管理的	应用内权限		,			
授权 权限系统	^	应用与人! 授权	员组织的授权关系	查看应用系统详细的操作日志 查看日志 查看同步记录		显否对应用开放系统API API Key API Secret	IP 白名单配置		管理的	应用内菜单与 Q限系统	功能权限				
审计	× ×	😽 GitLab	SAN ib	idaa 1251c9 in_sami3	Web应用				×			授权	详情 ▼		
设置	×	Same	SAM ins	irlo u251c gin_saml2	Web应用				×			授权	详情 ▼		
		S	SA	i 0ju251 ugin_sami1	Web应用				×			授权	详情 ▼		

## 管理员可以点击"添加账户关联"按钮手动为该应用添加一个关联子账户。

☆ 工作台					Q 搜索	费	用工单	备案	企业	支持	App	>_	Ū	Ä	? 简体
应用列表	長 / 子账户									_					
←子	账户									添	加账户;	关联	批調	時入	批量导出
Ŵ	子账户 子账户指的是在指定应 举例:IDaaS 中有主则 账户关联方式:在应用	2用系统中,用户会以什么身份进行 K户 张三(用户名 zhangsan),召 韵健时,如果选择了账户映射,即	订访问。主账户指的是 IDaaS 中的 企业的 BPM 应用系统中,这个5 即默认主账户和子账户完全一致,	9账户。在进行单点登录时,IDaaS 会 用户的用户名是 agoodman,即子账户 无需配置。如果选择了账户关联,则常	向应用系统传递对应的子账户,该 应为 agoodman,与主账户 zhani 要在这里进行手动的子账户创建#	好子账户需要在应用系统 igsan 进行关联。 和主子账户关联。	夺中存在且	可识别。							×
JWT															
主账	户 (账户名称)			Q											
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	

输入主账户的邮箱/手机号/账户名称以及子账户信息,点击保存按钮,即可成功添加一条账户关联。

添加账户关联		$\times$
* 主账户	gc_test	
* 子账户	gc_zzh	
	<b>保存</b> 返回	

### 1.2 手动批量绑定

管理员可以点击右上角"批量导入"按钮,从文件批量导入关联子账户。

应用列表 / 子账户							
← 子账户						添加账户关联	批星导入 批星导出
CAS(标准)							
主账户 (账户名)				٩			
主账户	子账户	显示名称	子账户密码	是否关联	审批状态	关联时间	操作
lintest	test	lintest	无	已关联	无	2019-06-18	删除
						共1条 〈 1	> 跳至 1 页

点击"批量导入"按钮后,跳转到导入账户关联页面,点击上传文件,选择需要上传的文件。(上传文件的格式可以参考下载的"账户关联格式范例文档")。

应用列表 / 账户关联 / <b>导入账户关联</b>
← 导入子账户
当前导入应用: 参考格式
★ 下载账户关联格式范例文档
请先下载账户关联格式范例文档,根据指定格式导入确保各字段类型正确无误,否则有可能导致导入失败。
导入文件 命 上传文件 请导入.xls文件
导入文件 返回

### A列是主账户名称, B列是子账户名称, 两个账户相互对应。

	А	В
1	主账户(IDP账户)	子账户(业务系统账户)

### 上传成功后,点击"导入文件"按钮。

应用列表 / 账户关联 / 导入账户关联

#### ← 导入子账户

当前导入应用:

	A	the last of the last of	

请先下载账户关联格式范例文档,根据指定格式导入确保各字段类型正确无误,否则有可能导致导入失败。

系统会自动检测上传文件的内容,并返回每一条记录的检测结果。管理员可以查看检测结果,并根据结果修

改文件,或移除某一条导入数据。确认无误之后,点击右上角"确定上传导入"即可实现批量添加应用子账户。

导	、账户关联			
	当前导入目标:			
	系统自动为您进行了数据校验,	请您先处理不合法数据才能进行上传导入操作,或者	f 重新上传。	
	请输入关键字进行查找		Q	确定上传导入
	主账户	子账户	校验结果	操作

### 2. 由用户申请绑定主子账户

首先使用普用户登录IDaas用户端, 登录方式请参考用户登录。

- 支持在用户门户首页申请绑定主子账户
- 支持在查看子账户页面进行绑定申请
- 2.1 在用户门户首页申请绑定

可以在首页的免登应用栏中直接点击对应应用

IDaaS统一认证身份平台					消息	gc_test - 切换语言 ~
欢迎·IDaaS	我的应用 搜索应用	Q				
主导航 ^	Web应用					
首页						
应用管理						
应用子账户	ר-ז	S			On	Ο
设置 ^		SAML	CAS	OAUTH	On	OAUTH
我的账户	阿里云RAM-用户SSO	SAML-sss	CAS(标准)-jenkins	OAuth2	表单代填	OAuth2-baidu
二次认证						
我的'冯恩 我的日志	(二) (二) (二) (二) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1	<b>C-D</b> 阿里元RAM:伯色SSO <b>米汤加限</b> / <sup>2</sup>	OA JVVT بالالالالالة:	JWT	GitLab	OAuth2-grafana
	移动应用 CA3(标注)-jenkins	J. J. MT	OALUTH OALUTH OALUTH2-garlana			

提示用户进行子账户的添加,用户输入子账户,等待管理员审批通过后即可添加该应用的子账户。

<b>提示</b> : 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*         gc_zzh           即您在此应用中的账户
提交账户关联

## 点击提交账户关联。

1	您提交的应用账户关联正在审批中,请等候公司管理员处理.							
Л Е	立用名称: JWT 主账户: gc_test							
-	子账户: gc_zzh							

## 2.2 在查看子账户页面申请绑定

也可以在导航栏中选择应用子账户	<sup>」</sup> ,点击右上角的'	"添加应用子账户"	进行子账户的添加。
-----------------	-----------------------	-----------	-----------

IDaaS统一认证身份平台						消息	gc_test -		切换语言
欢迎・IDaaS	应用子账户								
<b>主导航 ^</b> 首页	子账户列表	子账户审批		_					
应用子账户	添加应用子	<u> 搬</u> 戸 捜索 可用名称		٩					
设置 ^	应用图标	应用名称	审批状态	主账户	子账户	操作			
我的账户	OA	JWT	已通过	gc_test	gc_zzh	删	ŧ.		
二次认证我的消息	J	JWT	已通过	gc_test	gc_test	删	(k		
我的日志						共2条	< 1 >	跳至	1

用户选择添加子账户的应用,输入子账户,点击保存按钮。等待管理员审批通过,即完成了添加子账户。

### 应用身份服务

IDaaS统一认证身份平台				添加子账户		×
欢迎·IDaaS	節用子账户					
<b>主导航</b> ~ 首页	子账户列表 子账户审批			选择应用	JWT 講选择关單的应用	~
应用管理	添加应用子账户 搜索应用名称		٩	主账号		
应用子账户 设置 ^	应用關标 应用名称	审批状态	主账户	子账号	gc_zzh	
我的账户	TWL AO	已通过	gc_test		撮示:此应用子账户采用的是 账户关联 方式,您需要提供正确的用户名才能正确登录 到应用系统。	
二次认证 我的消息	JWT	已通过	gc_test		2000.000.00	
我的日志					0.47	

### 2.3 管理员进行审批

用户发出添加子账户的申请之后,管理员会收到添加子账户的申请。 管理员可以在审批中心下的子账户审批中对该用户添加子账户操作进行审批,同意申请后,用户即可成功添 加应用子账户。

应用列表									
添加应用	子账户审批 注册审批	子做小事能 注册事化 应用事能							
账户 ^									
机构及组	中世中心					×			
账户管理	■批中心是 IDa	aS 系统中管理员集中处理所有需要审批内容的功能	页面。当有待审批项出现时,会在左侧导航	记相应位置有数字气泡提示。					
分类管理		点登录时带给应用的身份标识。如果某应用设置其 白你可以每用了影白单占登录到应用系统由 法确	主子账户映射关系为「账户关联」时,用户	在尝试单点登录的时候,如果没有子账户,则会提 ====================================	交一个子账户绑定申请。由管理员在此处进	行审批。			
认证 ^	Фла <u>еция</u> , н		A 10465 HI-TRU-UTRU-UTRUES (80	27G/06/09 196.e					
认证源	主账户 (申请人)	子账户 应用名称	待审批 ~	Q. 搜索 重置 当前审批如果启用外	部审批流,请到外部审批平台进行处理!				
RADIUS									
证书管理	主账户 (申请人)	子账户	应用名称	申请时间	审批状态	操作			
授权 个	gc_test	gc_zzh	JWT	2021-06-25 12:05:18	待审批	查看详情 快速同意 快速拒绝 审批			
权限条统									
MCHINES.						共1条 〈 1 〉 跳至 1 页			
审计 ^									
進州日本									
20 Million	L								
具七官理 ^						P			
消息管理	P					8			
会话管理						•			
我的消息									

IDaaS统一认证身份平台					消息	gc_test + U 切换语言 >
欢迎·IDaaS	我的应用 搜索应用	Q				
主导航 ^	Webdit					
首页	WEDWIH					
应用管理						
应用子账户	<b>C</b> .7	S	C		On	
设置 ^		SAML	CAS	OAUTH	On	олитн
我的账户	阿里云RAM-用户SSO	SAML-sss	CAS(标准)-Jenkins	OAuth2	表单代填	OAuth2-baldu
二次认证						
我的消息						
我的日志	(as),	<b>[</b> -]	OA	J	👐 GitLab	0
	ム ~13 12.1511時間1			TWL		OAUTH
	表单代填_jwt 未添加账户	阿里云RAM-角色SSO 未添加账户	JWT	JWT	SAML_Gitlab	OAuth2-grafana
	移动应用					
	Cas	J	ОЛИТИ			
	CAS(标准)-jenkins	JWT	OAuth2-grafana			

若以上步骤全部成功完成,即完成添加应用子账户的功能,可以使用IDaaS账户进行单点登录应用。