

# 云联壹云 Meetup 15

## Part 2 : 多云统一账号管理 ( Cloud SSO )

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

2021-01 CEO 邱剑

# 目录

## CONTENTS

- 01 为什么需要Cloud SSO
- 02 方案工作原理
- 03 如何使用
- 04 典型应用场景

01

为什么需要  
Cloud SSO

## 多云场景下用户账号管理常见问题

- 员工忘了自己的云账号密码
- 员工设置了过于简单的密码
- 员工的权限设置过大
- 员工离职，清理其关联云账号

## 多云场景下用户账号管理复杂度分析

管理复杂度：

N

X

M

X

P

而且基本都是手工操作！

员工

几人~几百人

云账号

几个~十几个

权限

几十~几百

使用复杂度：

M

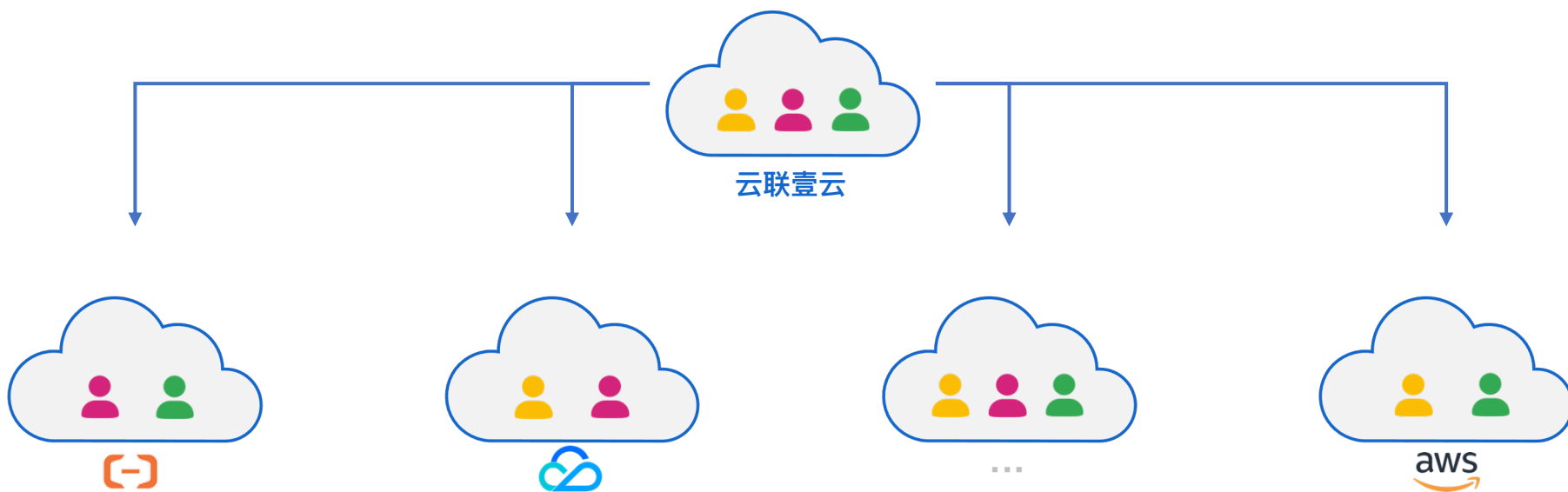
云用户账号和密码

02

## 方案工作原理

## 多云统一账号管理

多云统一账号管理：通过系统统一地管理企业员工在各个云上的账号及其权限



# 多云统一账号管理功能组件

## 1. 账号管理

定义每个用户在每个云账号的登录权限

## 2. 统一登录 (Cloud SSO)

实现用户免密登录到云控制台



## 多云统一账号管理收益

管理复杂度： $N \times 1 \times 1$   
员工数

使用复杂度： $1$   
个云联壹云账号

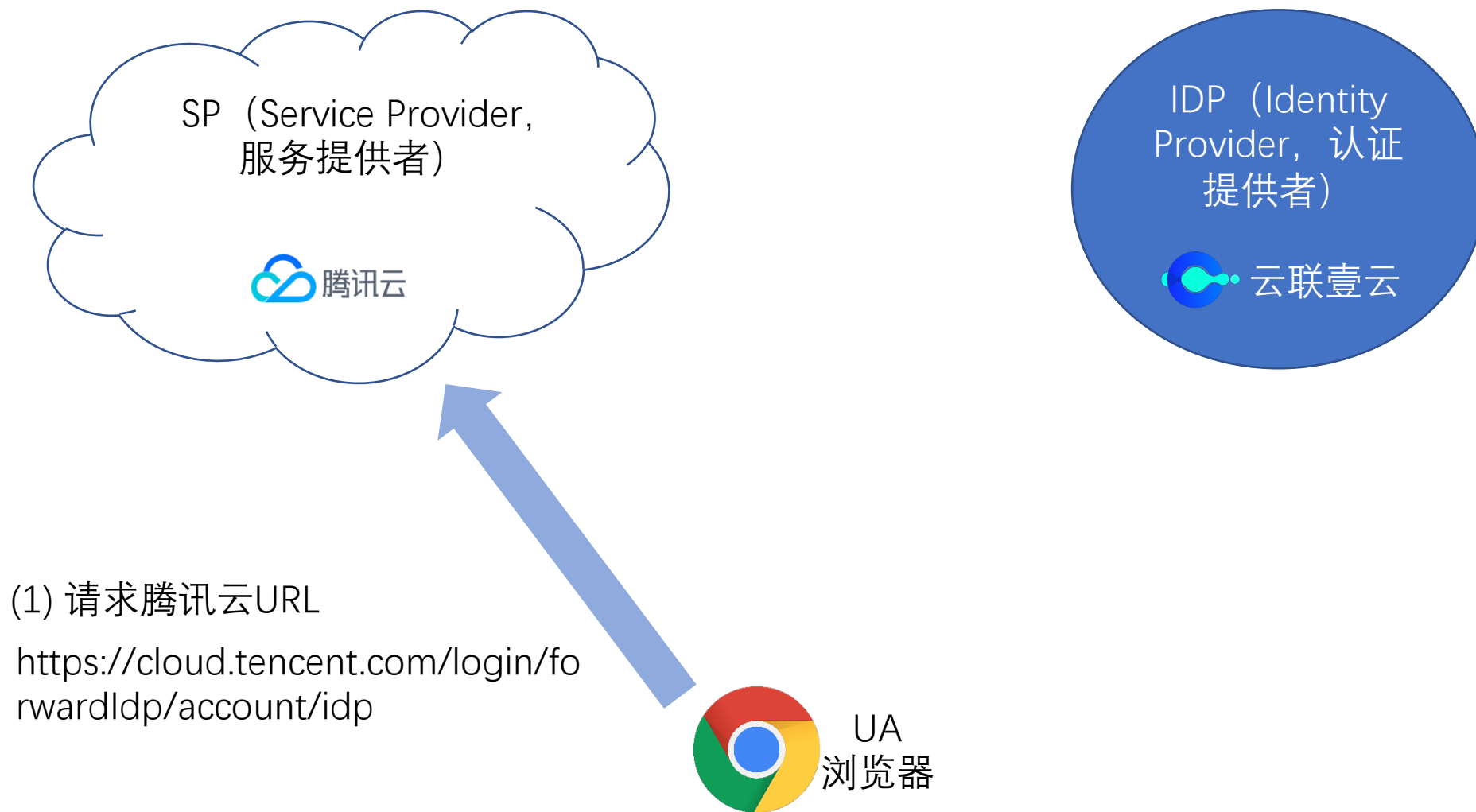
# SAML 2.0

Security Assertion Markup Language

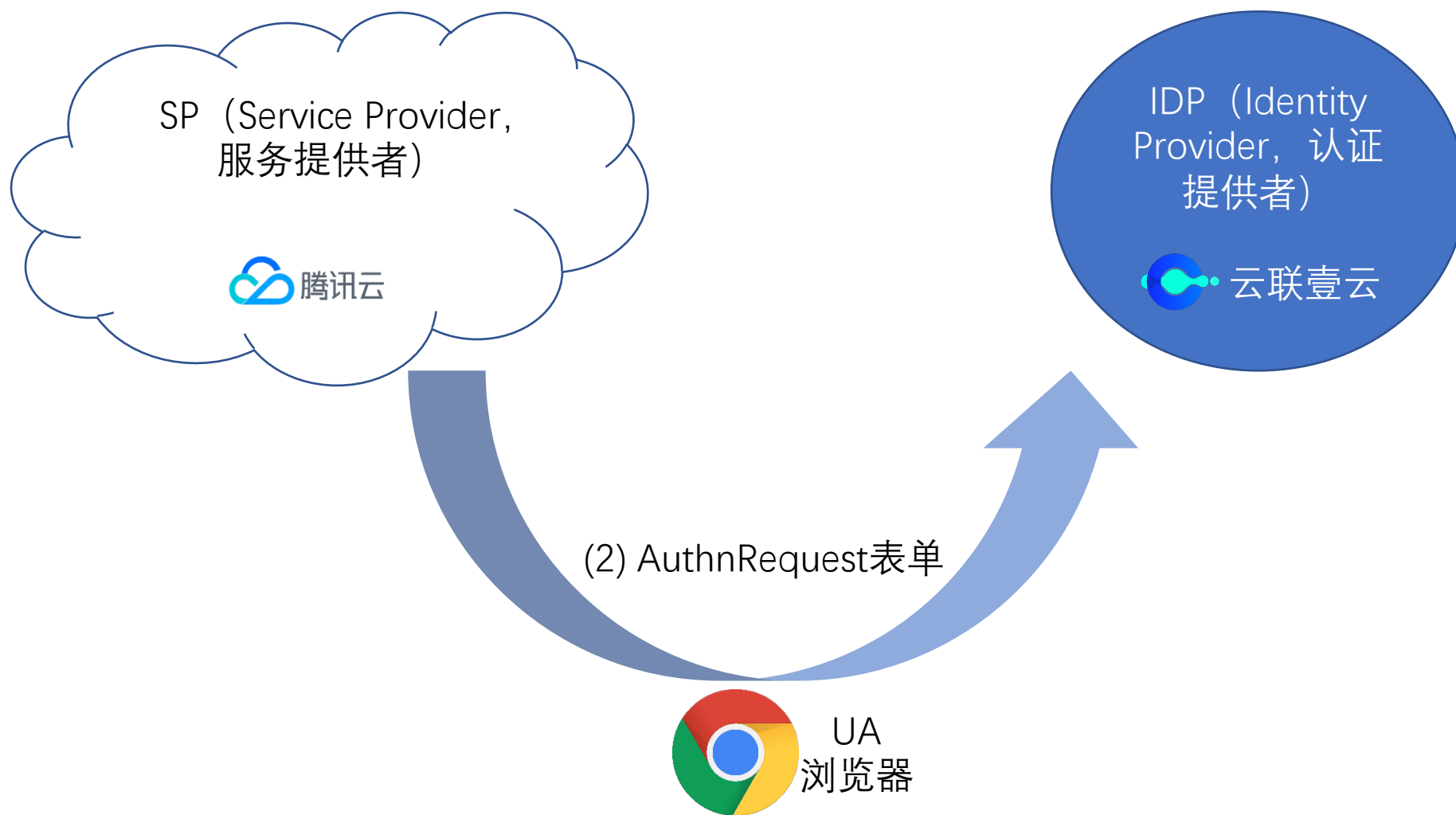
## SAML 2.0简介



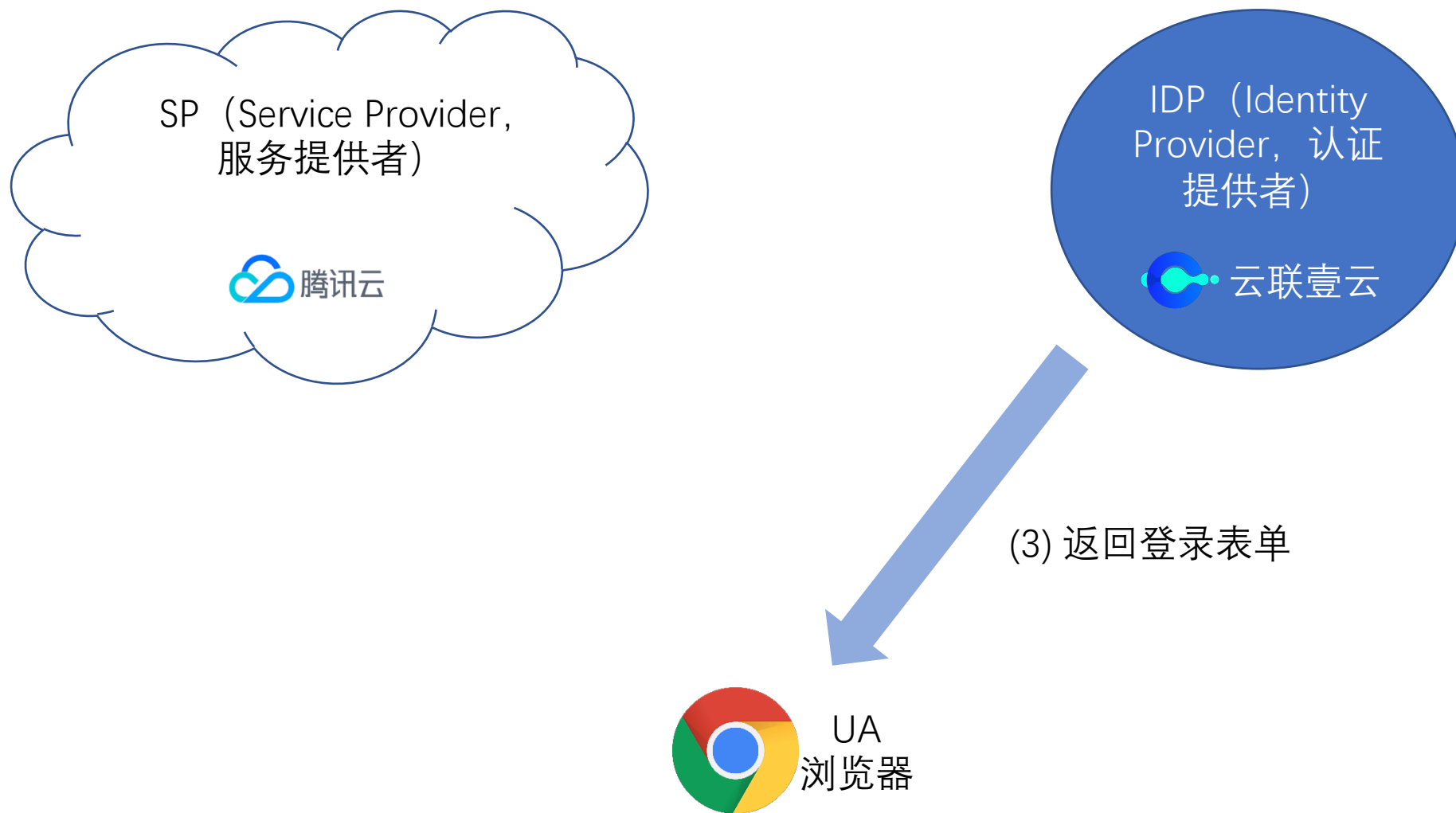
## SAML 2.0简介



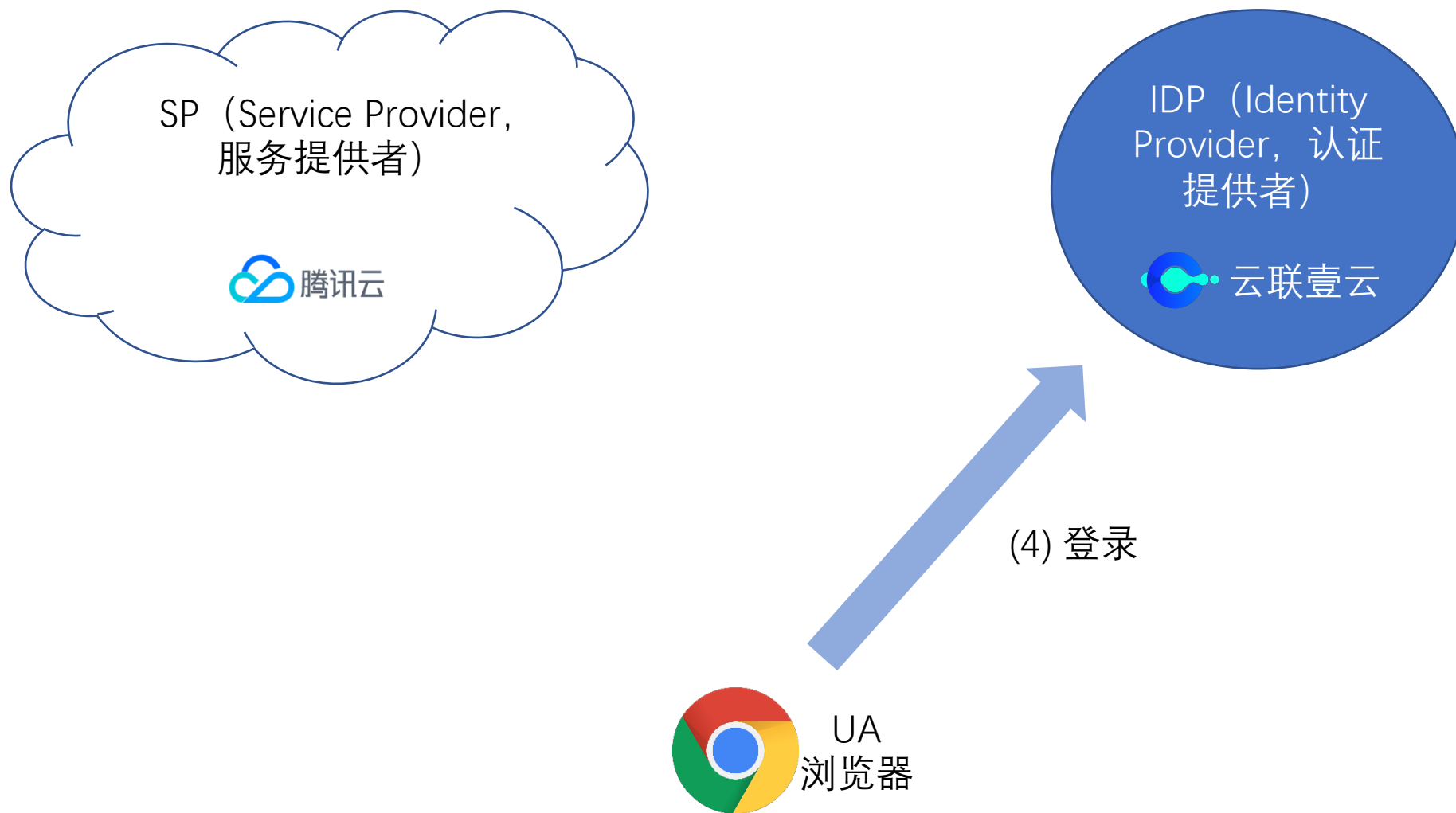
## SAML 2.0简介



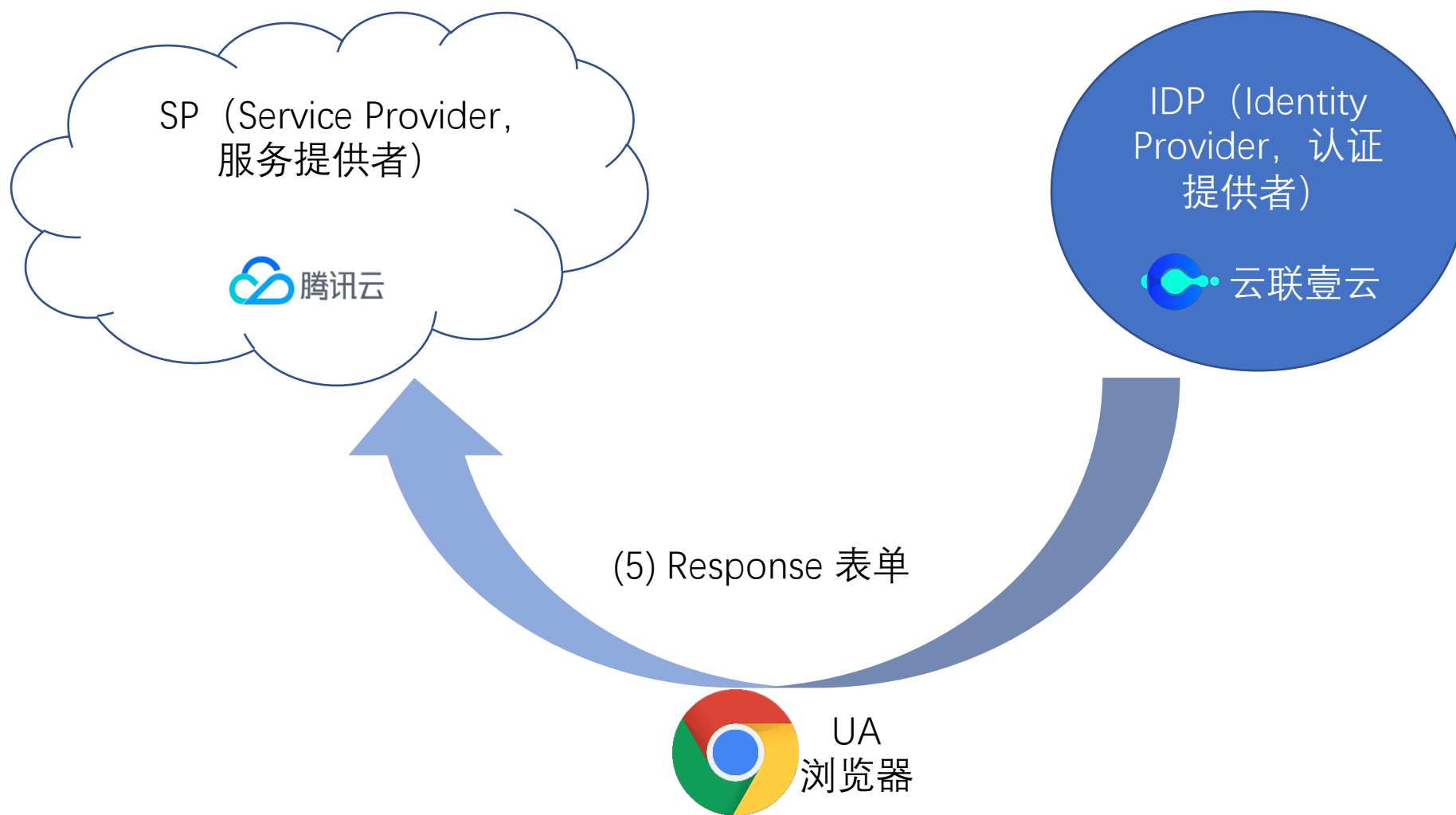
## SAML 2.0简介



## SAML 2.0简介

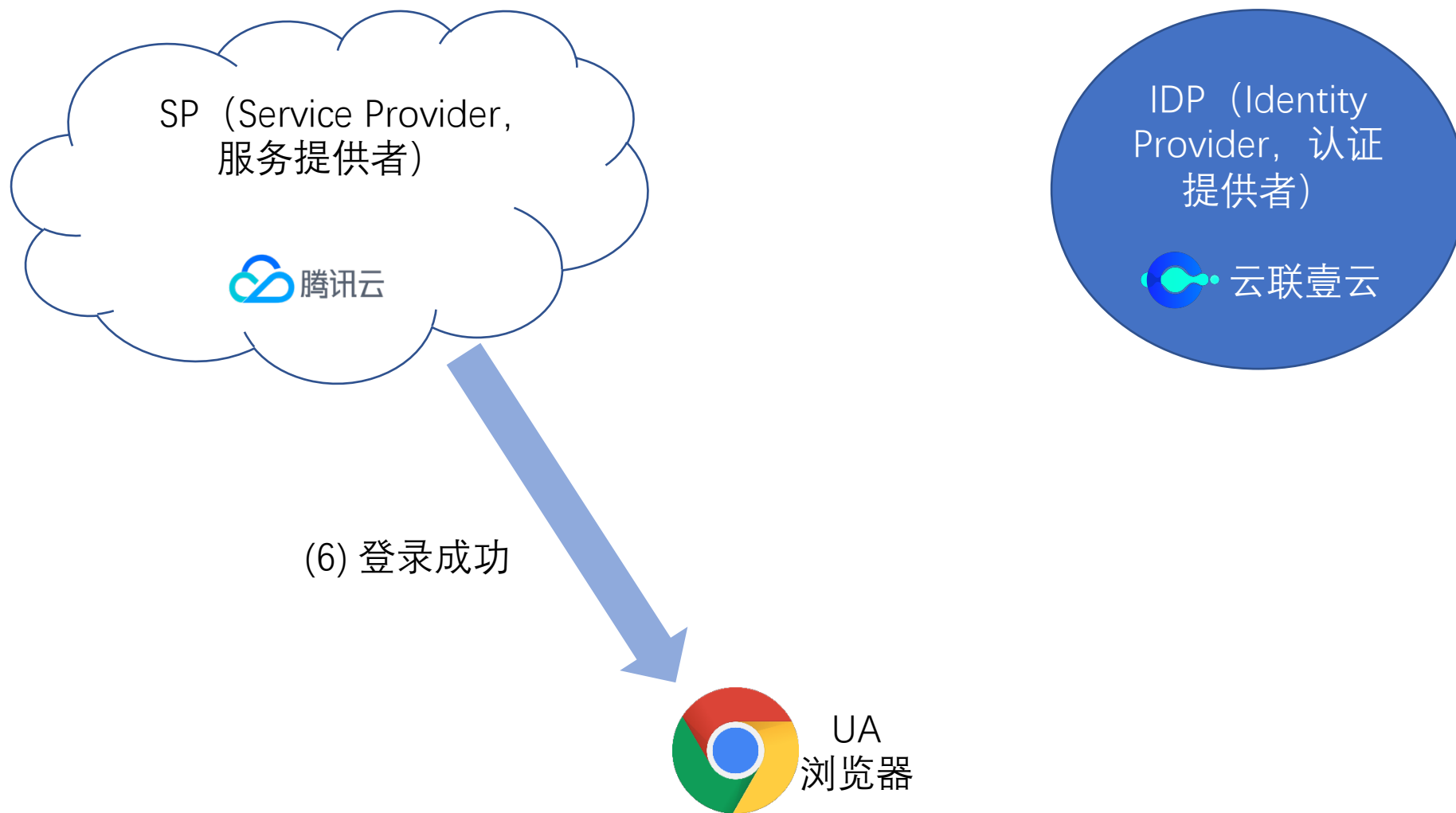


## SAML 2.0简介





## SAML 2.0简介



03

如何使用

# 1. 云上用户权限组管理——Cloud User Groups

多云管理

地域

区域

可用区

云账号

云账号

云用户组

代理

云上日志

标签

标签

调度

调度标签

调度策略

动态调度标签

云用户组

云用户组对应云上「用户组」,该页面可以对云用户组进行增删改查操作 我们会自动将所有云账号上的云用户组同步聚合,您可以使用该云用户组列表下的任意一个应用到其它同平台账号,不管该账号上是否有该云用户组都可以使用,我们会帮您自动同步,您无需操心

刷新

新建

删除

下载

设置

添加筛选项

<input type="checkbox"/>	名称	状态	权限	平台	共享范围	所属租户	操作
<input type="checkbox"/>	dev-1	● 可用	> 1个	aws	私有	wcl-test	同步状态 更多
<input type="checkbox"/>	admin-3	● 可用	> 1个	aws	私有	wcl-test	同步状态 更多
<input type="checkbox"/>	customer-1	● 可用	> 2个	aws	私有	wcl-test	同步状态 更多
<input type="checkbox"/>	readonlyazure	● 可用	> 1个	alicloud	私有	Default	同步状态 更多
<input type="checkbox"/>	test-1	● 可用	> 1个	alicloud	私有	Default	同步状态 更多
<input type="checkbox"/>	Security-Reader	● 可用	> 1个	alicloud	私有	Default	同步状态 更多
<input type="checkbox"/>	helanzhu	● 可用	> 1个	alicloud	私有	Default	同步状态 更多
<input type="checkbox"/>	test-azure-1	● 可用	> 2个	alicloud	私有	Default	同步状态 更多

## 1. 云上用户权限组管理——Cloud User Groups

[illegible]

## 2. 云账号开启Cloud SSO

The screenshot displays the Cloud SSO management interface. On the left, a dark sidebar contains navigation options: '多云管理' (Multi-Cloud Management), '地域' (Region), '区域' (Area), '可用区' (Availability Zone), '云账号' (Cloud Account), '云用户组' (Cloud User Group), '代理' (Proxy), '云上日志' (Cloud Log), '标签' (Tag), '调度' (Scheduling), '调度标签' (Scheduling Tag), '调度策略' (Scheduling Strategy), and '动态调度标签' (Dynamic Scheduling Tag). The '多云管理' option is highlighted with a red box.

The main content area shows a list of cloud accounts on the left, including 'AWS-wcl-test', 'qj-azure', 'yunion-china-az...', 'vc', 'qc-wcltest', 'OpenStacklyy', 'OpenStack', 'mj-test-01', and 'yos'. The '云账号' (Cloud Account) option is highlighted with a red box.

The '云账号' details page is displayed, showing tabs for '详情' (Details), '订阅' (Subscription), and '云用户' (Cloud User). The '详情' tab is active, showing the '基本信息' (Basic Information) section. A dropdown menu is open, showing options: '设置自动同步' (Set Auto Sync), '更新账号密码' (Update Account Password), '更新账单文件' (Update Bill File), '连接测试' (Connect Test), '设置优惠率' (Set Discount Rate), '设置共享' (Set Share), '设置代理' (Set Proxy), '开启免密登录' (Enable Passwordless Login), '启用' (Enable), '禁用' (Disable), and '删除' (Delete). The '开启免密登录' option is highlighted with a red box.

The '账号信息' (Account Information) section on the right shows the following details:

环境	金融云
健康状态	● 正常
优惠率	0%
余额	
虚拟机	0
宿主机	0

### 3. 本地用户的云上权限组分配

多云管理

地域

区域

可用区

云账号

云账号

云用户组

代理

云上日志

标签

标签

调度

调度标签

调度策略

动态调度标签

cephx

-

hw-test

-

qiujian-gcp

-

aws-test

-

ceph1

d 的

wp-ucloud

-

qcloud\_swordqiu

邱剑腾讯云

云账号

qcloud\_swordqiu

全量同步 更多

详情

订阅

免密登录用户

云用户

云用户组

云上项目

资源统计

操作日志

新建

删除

添加筛选项

名称	状态	云用户组	平台	所属云账号	操作
gaomingjiu	可用	test-qcloud		qcloud_swordqiu	删除
qx-test	可用	vpc-test		qcloud_swordqiu	删除
qiujian	可用	admin		qcloud_swordqiu	删除
quxuan	可用	vpc-test		qcloud_swordqiu	删除
gaoxianqi	可用	admin		qcloud_swordqiu	删除
houjiazong	可用	admin		qcloud_swordqiu	删除

<< < 1 / 1 > >>

20条/页

共 6 条记录

### 3. 本地用户的云上权限组分配

多云管理

地域

区域

可用区

云账号

云账号

云用户组

代理

云上日志

标签

标签

调度

调度标签

调度策略

动态调度标签

云账号

acloud\_swordaiu 全量同步 更多

新建免密登录用户

关联本地用户: 租户: wcl-test 项目: wcl-test2 用户: wcl-project

未加入项目的本地用户不支持关联云用户

\* 云用户组: 请选择

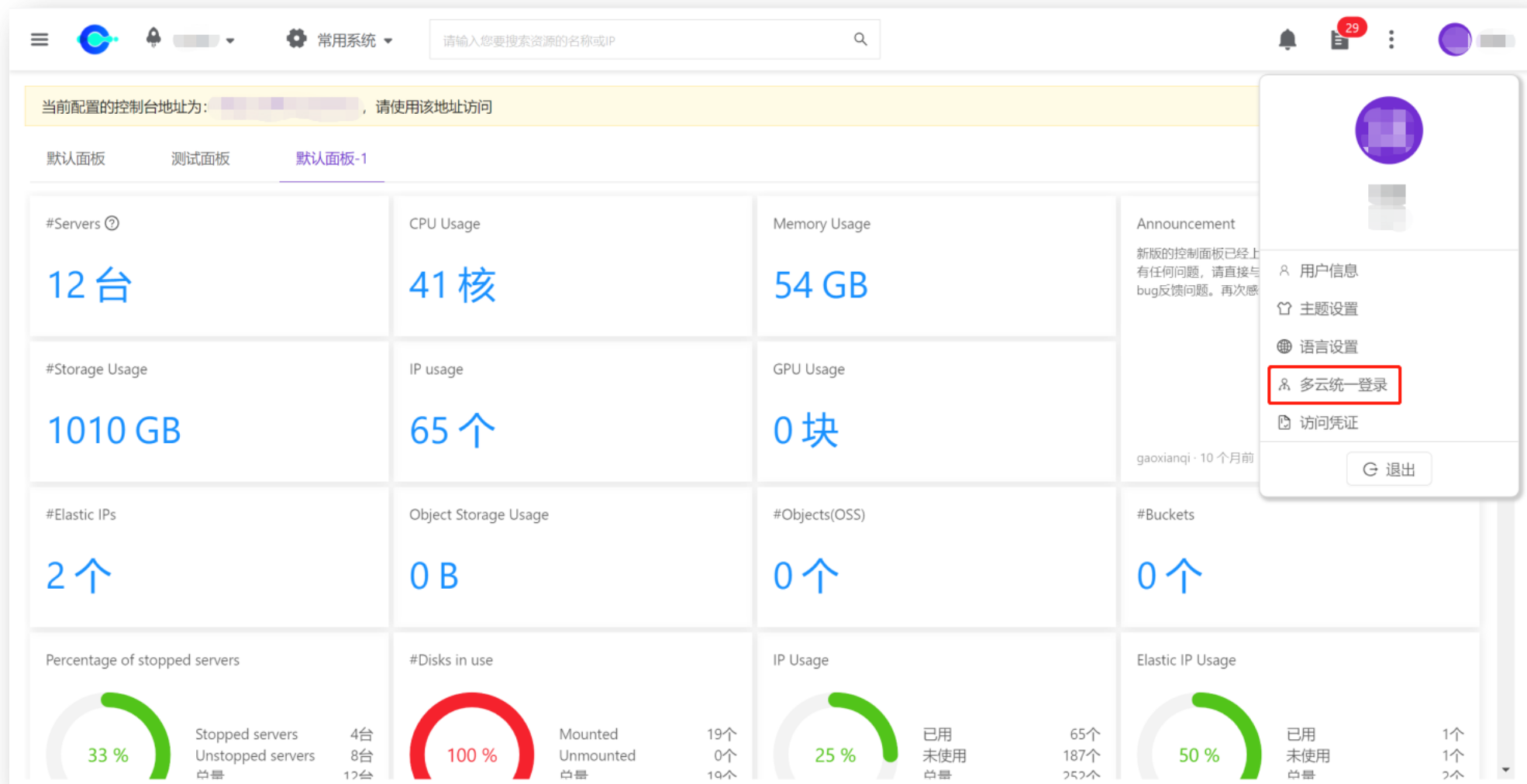
对应云上用户组，是权限的集合

确定 取消

houjiazong	可用	admin	qcloud_swordqiu	删除
------------	----	-------	-----------------	----

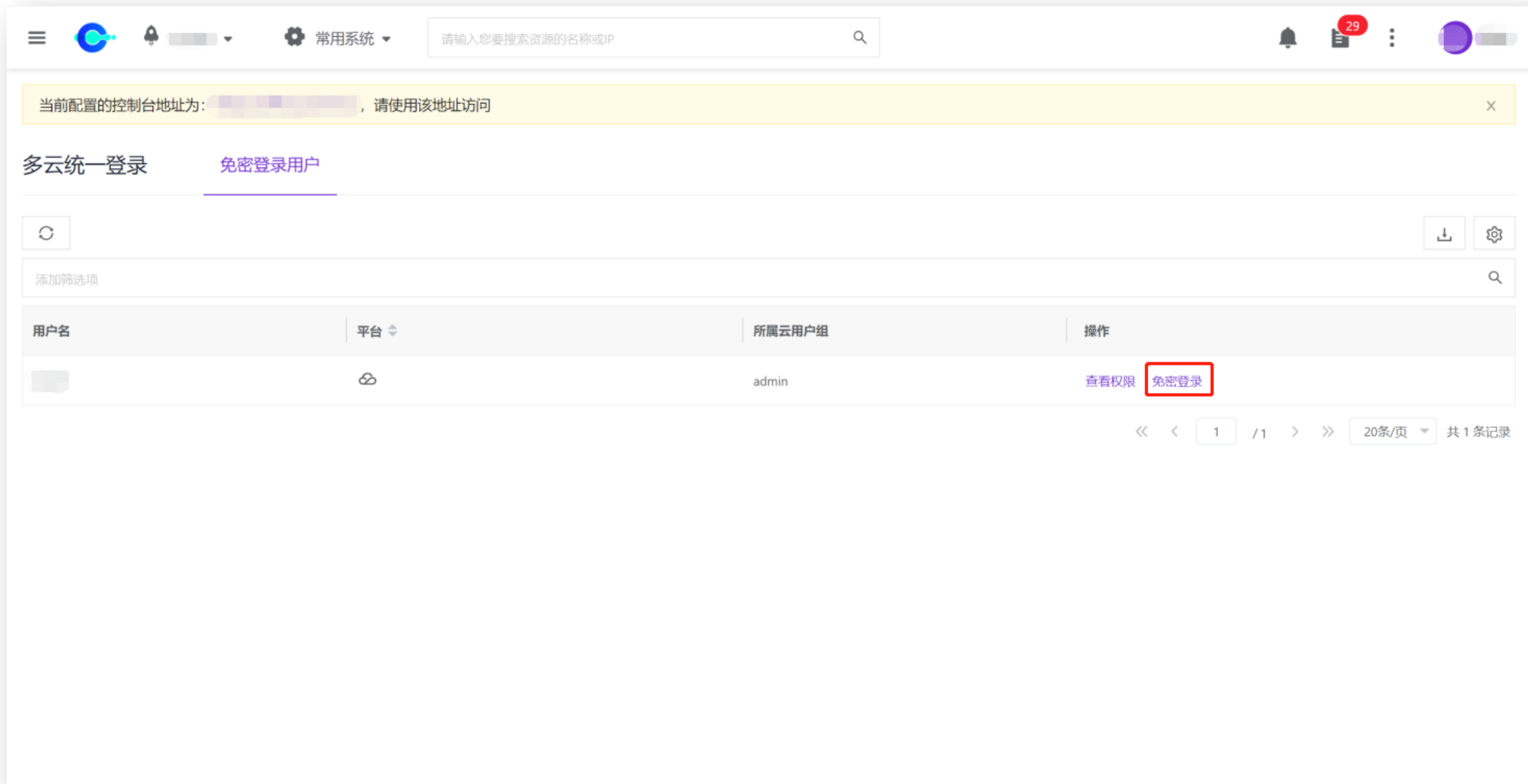
1 / 1 20条/页 共6条记录

## 4. 用户使用Cloud SSO登录公有云





## 4. 用户使用Cloud SSO登录公有云



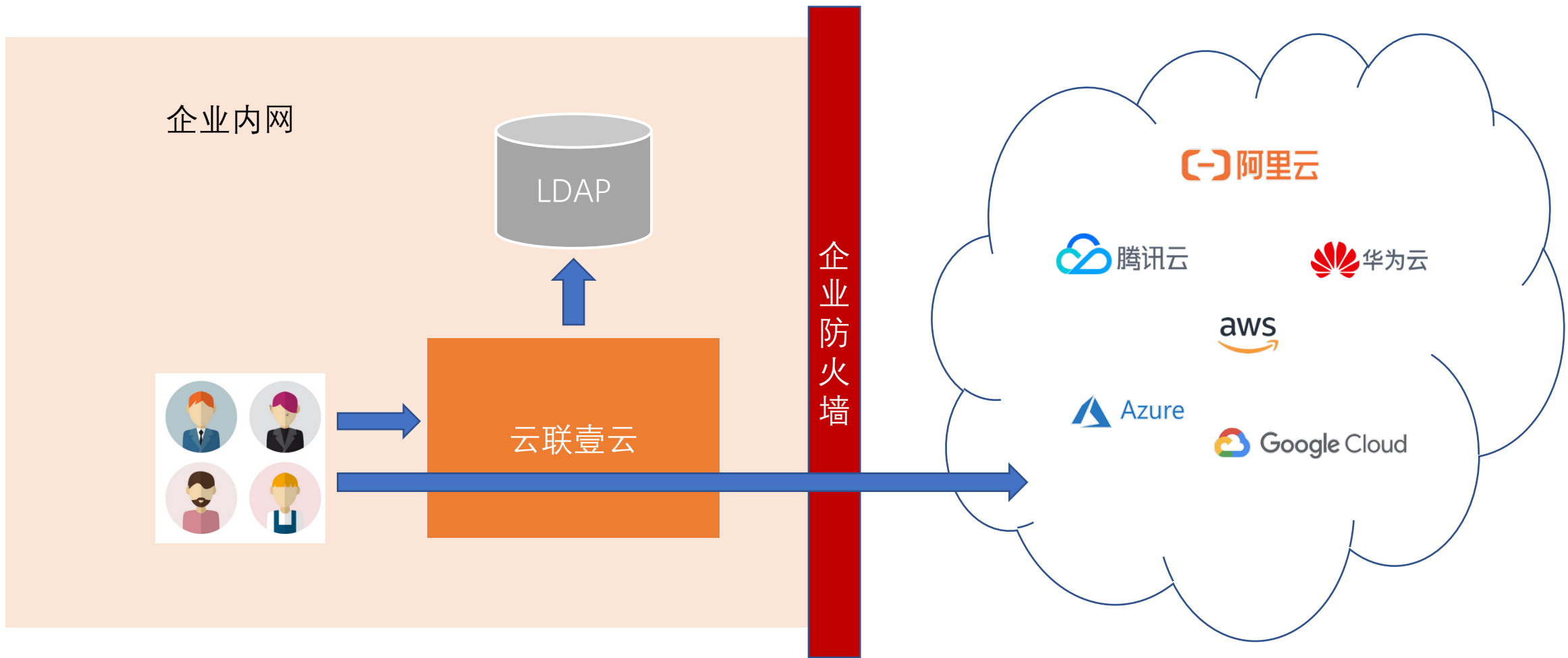
## Cloud SSO的支持情况

	 阿里云	 腾讯云	 华为云	 aws	 Azure	 Google Cloud
是否支持 Cloud SSO	支持	支持	支持	支持	支持	暂不支持
如何开启	自动开启	自动开启	自动开启	自动开启	手动开启	自动开启
登录载体	角色	角色	角色	角色	来宾用户	用户
其他限制条件					仅Azure国际区支持	需要开启GSuite和组织

04

典型场景

## 典型使用场景

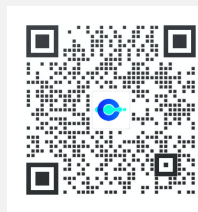


**Q&A**

# 2021 THANK YOU

云联壹云核心产品融合云 云联壹云 秉承：简单、开放、融合、智能的产品理念，能够帮助企业实现异构IT基础设施的全面云化、统一管理及成本优化，提高运维效率的同时，降低企业运营成本。

邱剑 2021-01-27



扫码进技术交流群



更多资讯关注我