访问管理

产品文档



腾讯云TCE

文档目录

- 产品简介
  - CAM概述
  - 产品功能
  - 应用场景
  - 使用限制
  - 支持CAM的产品
- 操作指南
  - 概览
  - 用户管理
    - 用户类型
    - 主账号
    - 子账号
      - 创建子用户
      - 子用户权限设置
      - 子用户安全凭证
        - 子用户登录
        - 为子用户重置登录密码
        - 为子用户设置安全保护
      - 子用户订阅消息
      - 删除子用户
    - 用户信息
    - 用户组
      - 新建用户组
      - 用户管理
      - 用户组权限设置
      - 删除用户组
    - 用户设置
      - 密码规则
      - 登陆策略
  - 策略管理
    - 相关定义
      - 权限
      - 策略
    - 授权指南
      - 创建自定义策略

- 授权管理
- 限制IP访问
- 语法逻辑
- 元素参考
- 语法结构
- 评估逻辑
- 资源描述方式
- 策略变量
- 生效条件
- 角色管理
- 角色概述
- 基本概念
- 创建角色
- 修改角色
- 删除角色
- 授权角色
- 为子账号赋予扮演角色策略
- 最佳实践
- 访问密钥
- 查看当前用户访问密钥
- 排除故障
- 如何根据故障反馈创建策略
- 企业认证登录管理
- 企业微信账号
- 运维手册
- 架构及模块说明
- 运维工具介绍
- 日常巡检
- 故障处理
- 应急预案
- 最佳实践
- 节点重启
- 扩容指导
- 备份恢复
- 参考信息

产品简介
CAM概述

最近更新时间: 2024-12-19 17:12:00

访问控制（Cloud Access Management，CAM）是云平台提供的Web服务，主要用于帮助客户安全管理云平台账户下资源的访问权限。用户可以通过CAM创建、管理和销毁用户(组)，并使用身份管理和策略管理控制其他用户使用云平台资源的权限。

产品功能

最近更新时间: 2024-12-19 17:12:00

CAM提供以下功能支持：

根账号资源的授权访问

可以将根账号的资源授权给其他人员，包括子账号和其他根账号，而不需要分享根账号相关的身份凭证。

精细化的权限管理

可以针对不同的资源授权给不同的人员不同的访问权限。例如可以允许某些子账号拥有CVM某台虚拟机的操作权限，而另一些账号或者根账号可以拥有某个地域的CVM操作权限等。这里的资源、访问权限、用户都可以批量打包。

最终一致性

CAM目前支持云平台的多个地域，通过复制策略数据实现跨地域的数据同步，虽然CAM策略的修改会及时提交，不过跨地域的策略同步会导致策略生效的延迟；同时CAM使用缓存来提高性能（目前是一分钟缓存），更新需要在缓存过期后生效。

版权所有：亿算云平台

应用场景

最近更新时间: 2024-12-19 17:12:00

企业子账号权限管理

企业内不同岗位的员工需要拥有该企业云资源的最小化访问权限。

场景：某个企业拥有很多云资源，包括CVM 、VPC实例、CDN实例、COS存储桶和对象等。该企业拥有很多员工，包括开发人员、测试人员、运维人员等。部分开发人员需要拥有其所在项目相关的开发机云资源的读写权限，测试人员需要拥有其所在项目的测试机云资源的读写权限，运维人员负责机器的购买和日常运营。当企业员工职责或参与项目发生变更，将终止对应的权限。

使用限制

最近更新时间: 2024-12-19 17:12:00

限制项	限制值
一个主账号中的用户组数	300
一个主账号中的子账号数	2000
一个子账号可加入的用户组数	300
一个用户组中的子账号数	300
一个主账号可创建的自定义策略数	1000
一个策略语法最大字符数	4096

> 注意：
>
> 1. 一个主账号可创建的自定义策略数包含COS自定义策略数。如果您遇到「超过自定义策略条数上限（上限为1500条）」提示且CAM自定义策略数未达到上限，可前往COS存储桶列表-控制台 ，单击存储桶名称进入权限管理处查看 ACL（Access Control List）数目是否超过上限。
> 2. 直接关联到一个用户、用户组的策略数包含COS自定义策略数。如果您遇到「关联策略失败」提示且CAM内关联策略数未达到上限，可前往COS存储桶列表-控制台 ，单击存储桶名称进入权限管理处查看 ACL（Access Control List）数目是否超过上限。

支持CAM的产品

最近更新时间: 2024-12-19 17:12:00

简介

访问管理已经支持对多数云产品服务进行权限管理。本文主要介绍支持访问管理CAM的产品服务的相关信息。具体维度包括授权粒度、控制台、根据标签进行授权、参考文档等。 以下列表分别罗列了云平台各大产品类别下已支持CAM的服务。 对表中信息进行如下定义：

- 服务：支持CAM的云服务的名称，单击链接至对应产品服务文档，方便您快速获取相关信息。
- 授权粒度：当前服务提供的最小授权粒度。

其中授权粒度按照粒度粗细分为服务级、操作级和资源级三个级别。

- 服务级：定义对服务的整体是否拥有访问权限，分为允许对服务拥有全部操作权限或者拒绝对服务拥有全部操作权限。
- 操作级：定义对服务的特定接口（API）是否拥有访问权限，例如：授权某账号对云服务器服务进行只读操作。
- 资源级：定义对特定资源是否有访问权限，这是最细的授权粒度，例如：授权某账号仅读写操作某台云服务器。
- 控制台：是否支持子账号通过控制台访问当前服务，“✓”表示支持，“-”表示暂不支持。
- 根据标签进行授权：当前服务是否支持通过标签进行权限管理，“✓”表示支持，“-”表示暂不支持。
- 参考文档：当前服务与CAM相关的文档链接，“-”表示暂无。

计算

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
云服务器	资源级	✓	✓	-	访问管理指南
容器服务	资源级	✓	-	-	访问管理指南
裸金属服务器	资源级	✓	-	-	-

存储

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
对象存储	资源级	✓	✓	-	访问管理指南
文件存储	资源级	✓	✓	-	访问管理指南
云硬盘	资源级	✓	✓	-	-
日志服务(cls)	资源级	✓	✓	-	-

网络

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
负载均衡	资源级	✓	✓	-	访问管理指南
私有网络	资源级	✓	✓	-	访问管理指南

数据库

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
分布式数据库（TDSQL）	资源级	✓	-	-	访问管理指南
云数据库（Redis）	资源级	✓	-	-	-
分布式云数据库（TBase）	资源级	✓	-	-	-
云数据库（MongoDB）	资源级	✓	-	-	-
时序数据库（CTSDB）	资源级	✓	-	-	-
关系型数据库（MariaDB）	资源级	✓	-	-	-
数据库管理（DMC）	资源级	✓	-	-	-
数据传输服务（DTS）	资源级	✓	-	-	-

管理与审计

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
访问管理	操作级	✓	-	-	访问管理指南
云审计	操作级	✓	-	-	-

监控与运维

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
云监控	操作级	✓	-	-	-
业务监控	服务级	✓	-	-	-

开发者工具

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
CODING DevOps	服务级	✓	-	-	-

公共服务

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
VPC域名解析（VPCDNS）	服务级	✓	-	-	-

大数据

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
Elasticsearch Service（CES）	服务级	✓	-	-	-

安全

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
堡垒机(dabs)	服务级	✓	-	-	-
数据加密服务(cloudhsm)	服务级	✓	-	-	-
主机安全(CWP)	服务级	✓	-	-	-
密钥管理系统(KMS)	服务级	✓	-	-	-
凭据管理服务(SSM)	服务级	✓	-	-	-
Web应用防火墙(WAF)	服务级	✓	-	-	-
数据安全审计	服务级	✓	-	-	-
敏感数据处理	服务级	✓	-	-	-
云防火墙（CFW）	服务级	✓	-	-	-

中间件

服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
微服务平台(TSF)	服务级	✓	-	-	-
消息队列(TDMQ)	服务级	✓	-	-	-
消息队列(CKafka)	服务级	✓	-	-	-
API网关(APIGW)	服务级	✓	-	-	-

运营平台

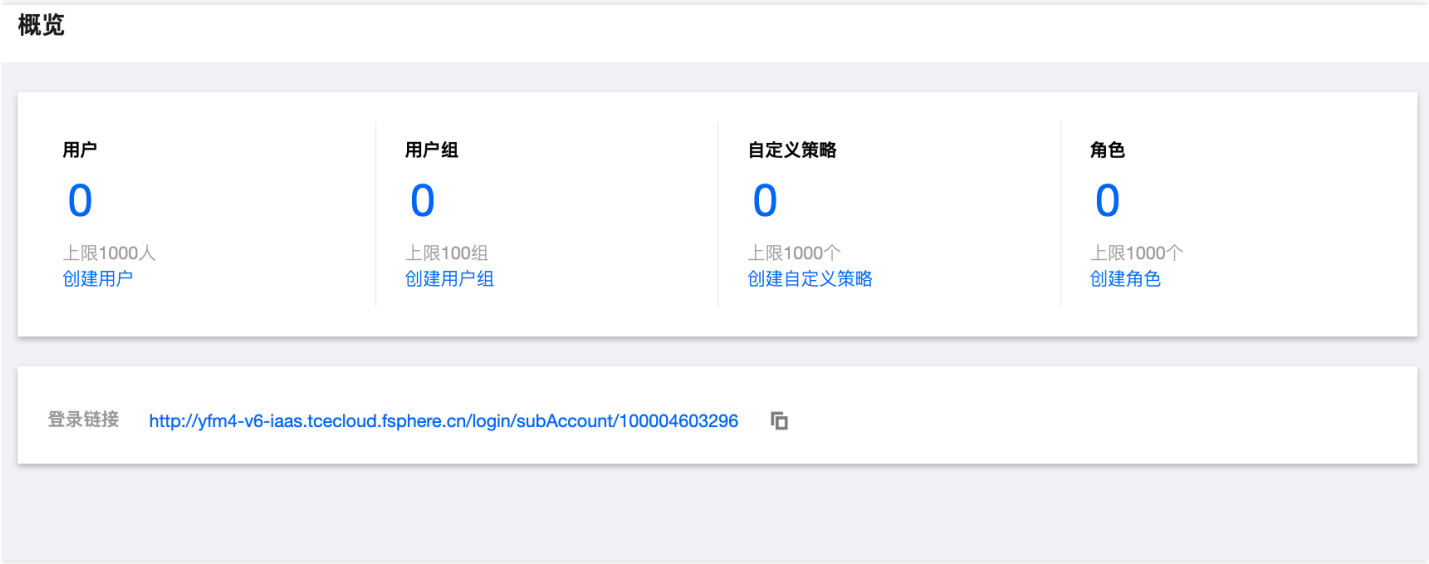
服务	授权粒度	控制台	根据标签进行授权	服务角色	参考文档
云审计	服务级	✓	-	-	-
访问管理	服务级	✓	-	-	-
标签	服务级	✓	-	-	-

操作指南

概览

最近更新时间: 2024-12-19 17:12:00

登录访问管理控制台，并在左侧导航栏中，选择【概览】，进入概览页面，显示用户、用户组、自定义策略、角色数量，和创建入口以及访问管理指引。



用户管理
用户类型

最近更新时间: 2024-12-19 17:12:00

CAM 用户为您在云平台中创建的一个实体，每一个CAM用户仅同一个云账户关联。您注册的云账号身份为**主账号**，您可以通过用户管理来创建拥有不同权限的**子账号**协助您。子账号的类型分为子用和消息接收人。

|

账号类型	主账号	子账号	
		子用户	消息接收人
定义	拥有云所有资源，可以任意访问其任何资源。 不建议使用主账号对资源进行操作，应创建子账号并按照最小权限原则赋予策略，使用权限范围有限的子账号操作您的云资源。	由主账号创建，完全归属于创建该子用户的主账号。	仅拥有消息接收功能。
控制台访问	✔	✔	-
编程访问	默认已拥有全部策略	✔	-
策略授权	✔	✔	-
消息通知	✔	✔	✔

主账号

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍主账号权限设置，消息接收，您可以通过以下步骤了解主账号权限以及如何修改消息接收方式。

前提条件

已注册云平台账号即主账号。

操作步骤

主账号无需授权

主账号默认拥有账号下云平台所有资源，无需授权，可以任意访问其任何资源。因此，不建议您使用主账号对资源进行操作，应创建子账号并按照最小权限原则赋予策略，使用权限范围有限的子账号操作您的云资源。

主账号消息接收

您注册云平台主账号时登记的安全手机、安全邮箱将同时作为初始消息接收方式。若您在账号中心 > 控制台内修改了安全手机或安全邮箱，您在访问管理（CAM）> 控制台用于云平台消息通知的联系手机或联系邮箱不会同步修改。

> 注意：为避免您因消息遗漏造成的损失，请您及时前往【访问管理】控制台确认用于消息订阅的联系手机或联系邮箱是否符合预期。

子账号
创建子用户

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何创建及设定子用户的权限，子用户将在获得的权限范围内管理主账号下的资源。

操作指南

通过控制台创建

您可以通过登录云控制台，通过控制台创建子用户并设定权限。

1. 登录访问管理控制台，并在左侧导航栏中，选择【用户管理】>【用户】，进入用户页面。
2. 在用户页面，单击【新建用户】，弹出【选择新建用户类型】对话框，选择【子用户】，进入【新建子用户】页面。
3. 在填写用户信息页面，在“设置用户信息”下填写用户名（必填）、昵称、手机、邮箱信息。

> 说明 - 单击【新增用户】可一次最多创建10个用户。

- 因子用户登录使用用户名，用户名一经确定将无法更改。

4. 在“访问类型”下设置子用户的访问方式。

- 编程访问：启用SecretId和SecretKey，子用户将通过云API、SDK和其他开发工具管理权限范围内的主账号资源。
- 云平台管理控制台访问：启用密码，子用户将通过登录到云控制台方式管理权限范围内的主账号资源。

> 说明：为了保证您的账号安全，建议您开启登录保护和操作保护。

5. 设置【控制台密码】、【需要重置密码】、【登录保护】、【操作保护】。
6. 单击【创建】，创建子用户。创建成功后，系统自动进入【设定权限】页面。
7. 在【设定权限】中，可以选择：

- 添加到现有用户组：新建用户组，并将子用户添加进来，或者选择加入现有用户组。

- 复制现有用户权限：复制现有用户，使得当前用户具有已选择用户的权限。
- 从策略列表中授权：选择策略，给当前子用户添加对应的策略权限。

8. 单击【下一步：完成】，进入设置用户权限页面。
9. 在设置用户权限页面，根据您的实际需求，选择不同的方式为当前新建的子用户设定权限，关联策略后子用户将获得策略描述的权限。

- 添加至现有用户组：把子用户添加到组是按工作职能来管理用户权限的最佳做法，您可以通过随组关联获得权限。将子用户添加到现有用户组或新建用户组，子用户可以随组关联到该组附加的策略。
- 复制现有用户权限：通过复制现有用户的权限为子用户关联策略，单击【复制现有用户权限】，勾选需要复制的用户，子用户可以关联到被复制用户附加的策略。
- 从策略列表中授权：单击【从策略列表中授权】，勾选需要关联的策略。

10. 单击【下一步：完成】。
11. 在完成页面，单击【完成】完成创建子用户操作，进入提示新建子用户成功页面。
12. 进入提示新建子用户成功页面，您可以通过以下方法获取子用户信息。

- 单击【下载安全凭证】通过 excel 文件将部分信息保存至本地。

通过API创建

您可以通过访问密钥调用 AddUser 接口添加子用户并设定权限。

子用户权限设置

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何授权和解除子用户关联的策略，子用户将在获得的权限范围内管理主账号下的资源。

操作步骤

为子用户授权关联策略

直接关联

您可以直接为用户关联策略以获取策略包含的权限。

1. 登录访问管理控制台，选择【用户管理】>【用户】，进入 用户管理页面。
2. 在用户管理页面，点击用户，进入用户详情页。
3. 单击【已经关联的策略】可以查看已经关联的策略。
4. 点击关联策略，在弹出的策略列表选择策略。
5. 单击【确定】完成直接为子用户授权关联策略操作。

随组关联

您可以将用户添加至用户组，用户将自动获取该用户组所关联策略的权限，通过此种方法获取的策略类型为随组关联。如需解除随组关联策略，需将用户移出相应用户组。

1. 登录访问管理控制台，选择【用户管理】>【用户组】，进入 用户管理页面。
2. 在用户组管理页面，点击用户组，进入用户组详情页。
3. 单击【已经关联的策略】可以查看已经关联的策略。
4. 点击关联策略，在弹出的策略列表选择策略。
5. 单击【确定】完成直接为用户组授权关联策略操作。

为子用户解除关联策略

直接解除子用户关联策略

您可以直接解除用户关联的策略以解除用户关联的权限。

1. 登录访问管理控制台，选择【用户管理】>【用户】，进入用户组管理页面。
2. 在用户管理页面，点击用户，进入用户详情页。
3. 单击【已经关联的策略】可以查看已经关联的策略。

4. 点击解除策略。
5. 单击【确定】完成直接为子用户授权解除策略操作。

从组中移出用户

您可以从组中移出用户以解除用户关联的策略

1. 登录访问管理控制台，选择【用户管理】>【用户组】，进入用户组管理页面。
2. 在用户组管理页面，点击用户组，进入用户详情页。
3. 单击【已经关联的策略】可以查看已经关联的策略。
4. 点击解除策略。
5. 单击【确定】完成直接为子用户授权解除策略操作。

子用户安全凭证
子用户登录

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何登录子用户和企业微信子用户，登录成功后子用户将在权限范围内管理主账号下的资源。

操作步骤

子用户登录

通过账号、密码登录

您可以通过以下步骤使用账号、密码的方式登录 自定义创建的子用户，登录成功后，可在设置的权限范围内管理主账号下的资源。

1. 进入 子用户登录 页面进行账号登录。
2. 在子用户登录页面，输入主账号 ID、子用户名、登录密码信息，

   > 主账号 ID 即子用户所属主账号 ID。账号 ID（例如：100001234567）是账号在云平台的唯一标识，请联系主账号在 账号信息处查看。

3. 单击【登录】，完成通过账号、密码方式登录子用户操作。

为子用户重置登录密码

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何修改子用户密码，修改之后可以通过新的密码登录子用户管理主账号下资源。

操作步骤

1. 在【用户管理】>【用户】中选择需要修改密码的子用户，选择具体【用户名称】，进入用户详情页。
2. 在用户详情页中选择【安全设置】>【控制台密码】，单击【管理密码】。
3. 在弹出的【管理控制台访问】窗口中，设置当前用户密码。

- 若您当前子用户需要通过登录控制台访问云，请将【控制台访问】设置为【启用】。
- 若您需要为子用户设置新密码，您可以通过以下两种方式。
  - 若您在【控制台密码】中选择【自动生成的密码】，系统会自动生成控制台登录密码。您可以复制保存，如有需要可以单击【下载.csv】保存密码。
  - 若您在【访问密码】中选择【自定义密码】，输入您为该子用户设置的控制台登录密码。
- 若您需要当前用户自行重置密码，可勾选【用户必须在下次登录时重置密码】，子用户在下次登录成功后将被要求重新设置控制台登录密码。

为子用户设置安全保护

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何开启和关闭子用户的安全保护，子用户将根据设置判断是否进行安全验证。

操作步骤

为子用户开启安全保护

1. 登录访问管理控制台，并在左侧导航栏中，选择【用户管理】>【用户】，进入用户管理页面。
2. 在用户管理页面，选择需要设置安全保护的子用户。
3. 单击【用户名称】，进入用户详情页面。
4. 在用户详情页面，单击【安全设置】，进入安全管理页面。
5. 在安全管理页面，单击身份安全操作栏下的【管理MFA】。
6. 在弹出的身份安全窗口中，勾选需要开启的保护类型，为当前子用户开启相应的安全保护。
7. 单击【确定】，完成为子用户开启安全保护操作。

为子用户关闭安全保护

1. 登录访问管理控制台，并在左侧导航栏中，选择【用户管理】>【用户】，进入用户管理页面。
2. 在用户管理页面，选择需要设置安全保护的子用户。
3. 单击【用户名称】，进入用户详情页面。
4. 在用户详情页面，单击【安全设置】，进入安全管理页面。
5. 在安全管理管理页面，单击身份安全操作栏下的【管理MFA】
6. 在弹出的身份安全窗口中，勾选需要关闭的保护类型，为当前子用户关闭相应的安全保护。
7. 单击【确定】，完成为子用户关闭安全保护操作。

版权所有：亿算云平台

子用户订阅消息

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何为子用户验证消息渠道以及设置订阅消息。如需子用户接收消息，需子用户验证通过消息渠道，为其订阅消息后该用户已验证通过的消息渠道即可接收相关的消息提醒。

操作指南

设置订阅消息

1. 进入消息中心，点击消息订阅
2. 选择消息类型
3. 点击添加接收人
4. 在弹出的“添加接收人”窗口，勾选需订阅的的接收人/接收组。
5. 单击【确定】，完成设置订阅消息操作。

删除子用户

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何删除单个或者多个子用户，删除之后，子用户将不再拥有该主账号的管理权限。

前提条件

已登录访问管理控制台，选择【用户管理】>【用户】，进入用户管理页面。

操作步骤

删除单个子用户

1. 在用户管理页面，找到需要删除的子用户。
2. 单击右侧操作列的【删除】。
3. 在弹出的删除用户窗口，确认当前子用户下的 API 密钥已禁用且删除，详细请参考访问密钥。
4. 单击【确认删除】，完成删除单个子用户操作。

删除多个子用户

1. 在用户列表管理页面，左侧勾选需删除的子用户。
2. 单击左上方的【删除】。
3. 在弹出的删除用户窗口，确认已勾选子用户下的 API 密钥已禁用且删除，详细请参考 访问密钥。
4. 单击【确认删除】，完成删除多个子用户操作。

用户信息

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何查看和修改子账号用户名、备注、手机等信息。

查看用户信息

1. 登录访问管理控制台，选择【用户管理】>【用户】，进入用户管理页面，找到需要查看用户信息的子账号。
2. 单击【用户名称】，进入用户详情页面。
3. 可在页面上方查看当前子账号的用户信息（含用户名、备注、手机、邮箱、是否允许微信通知）。

修改用户信息

1. 登录访问管理控制台，选择【用户管理】>【用户】，进入用户管理页面，找到需要修改用户信息的子账号。
2. 单击【用户名称】，进入用户详情页，单击右上角【编辑】。
3. 在弹出的编辑信息窗口，修改相应的用户信息。
   - 用户名：修改当前用户的用户名，子用户因登录使用用户名，无法修改。
   - 联系手机：修改当前子账号绑定手机信息，该手机可以用于接收主账号消息通知及敏感操作前的身份验证。
   - 联系邮箱：修改当前子账号绑定邮箱信息，该邮箱可以用于接收主账号消息通知。
4. 单击【确定】，完成修改用户信息操作。您可以通过修改之后的用户名、手机、邮箱在 用户列表管理页面，搜索到您的子账号。

用户组

新建用户组

最近更新时间: 2024-12-19 17:12:00

新建用户组

1. 登录访问管理控制台，选择【用户管理】>【用户组】，进入用户组管理页面。
2. 单击【新建用户组】，进入填写用户组信息页面。
3. 在填写用户组信息页面，填写用户组名和备注，其中用户组名为必填项。

   > 说明： 在用户组列表中您可以搜索用户组名或备注，在众多用户组中快速准确定位到对应的用户组。

4. 单击【确定】，创建用户组成功。
5. 单击新建的用户组名称，进入设置用户组信息页面。
6. 在设置【已关联的策略】页面，单击【关联策略】，进入管理策略页面。
7. 勾选需要授权的策略（可多选），单击【确定】，即可关联策略成功。
8. 在【已关联的策略】，您可以查看用户组的相关设置，如有误可点击【解除】修改。

关联文档

如果您想了解如何通过用户组管理子用户进行分组授权，请参阅 用户管理、用户组权限设置。 如果您想了解如何创建子用户，请参阅 自定义创建子用户。

用户管理

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何新为用户组添加或者删除单个、多个用户。

前提条件

已登录访问管理控制台，选择【用户管理】>【用户组】，进入用户组页面。

操作步骤

为用户组添加用户

单个用户组添加用户

1. 在用户组页面，找到要添加用户的用户组。
2. 单击右侧操作列的【添加用户】。
3. 在弹出的添加用户窗口，勾选要添加的用户。
4. 单击【确定】，完成为用户组添加用户操作。

多个用户组添加用户

1. 在用户组页面，左侧勾选需要添加的用户组。
2. 单击左上角【添加用户】。
3. 在弹出的添加用户窗口，勾选要添加的用户。
4. 单击【确定】，完成为用户组添加用户操作。

为用户组删除用户

为用户组删除单个用户

1. 在用户组页面，找到要删除用户的用户组。
2. 单击用户组名称，进入用户组详情页。
3. 在用户组详情页，单击【已添加的用户】，进入用户列表页面。
4. 在用户列表页面找到要删除的用户，单击右侧操作列的【移出该组】。
5. 单击【移出用户】，完成为用户组删除单个用户操作。

为用户组删除多个用户

1. 在用户组页面，找到要删除用户的用户组。
2. 单击用户组名称，进入用户组详情页。
3. 在用户组详情页，单击【已添加的用户】，进入用户列表页面。
4. 在用户列表页面，勾选需要删除的用户。
5. 单击【移出用户】>【确认移出】，完成为用户组删除多个用户操作。

用户组权限设置

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何授权和解除用户组关联的策略，用户组下的子账号将在获得的权限范围内管理主账号下的资源。

前提条件

已登录访问管理控制台，选择【用户管理】>【用户组】，进入用户组管理页面。

操作步骤

为用户组添加策略

1. 在用户组管理页面，单击用户组名称，进入用户组详情页。
2. 在用户组详情页，单击【已关联的策略】，进入权限管理页面。
3. 在权限管理页面，单击【关联策略】。
4. 在弹出框勾选要添加的策略（可多选），单击【确定】，完成为用户组添加策略操作。

为用户组解除策略

1. 在用户组管理页面，单击用户组名称，进入用户组详情页。
2. 在用户组详情页，单击【已关联的策略】，进入权限管理页面。
3. 在列表中找到需要解除的策略，单击右侧的【解除】。
4. 确认无误后单击【确认解除】，完成为用户组解除策略操作。

版权所有：亿算云平台

删除用户组

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何删除用户组，删除之后，用户组下的子账号将不再拥有通过用户组获得的权限。

操作步骤

删除单个用户组

1. 选择【用户管理】>【用户组】，进入用户组管理控制台页面。
2. 在用户组管理控制台页面，找到需删除的用户组。
3. 单击右侧操作列的【删除】，完成删除用户组的操作。

用户设置
密码规则

最近更新时间: 2024-12-19 17:12:00

操作场景

本章节介绍如何设置子用户的密码有效期。

操作步骤

> 说明
>
> - 该步骤所设定的密码规则仅适用于使用密码登录的子用户。
> - 登录密码失效后子用户将无法通过其他登录方式进行登录，须重置登录密码。

1. 选择【用户管理】> 【用户设置】，进入安全设置页面。
2. 点击【密码规则设置】模块的编辑按钮，可以修改密码规则、密码长度、密码的有效期限以及密码重复次数。

- 密码规则：至少包含大写字母、小写字母、数字、特殊规则中的两项密码规则
- 最短密码长度：默认最短10个字符，最长可设置32个字符
- 密码有效期：0天表示不限制，最长可设置 365 天
- 重复限制：限制新密码与历史密码的重复，默认与前1次不重复。（最大24次密码不重复）
- 密码黑名单：用户设置密码，禁止包含黑名单中设置的字符串，最多可设置10个

3. 单击【确定】按钮完成密码复杂度设置。从上一次修改密码开始计算，到达有效期需要重置密码。

登陆策略

最近更新时间: 2024-12-19 17:12:00

本章节介绍如何设置子用户的会话超时时间。

前提条件

必须使用主账号或者有管理员权限的子账号登录租户端。

操作步骤

1. 选择【用户管理】> 【用户设置】，进入用户设置页面。
2. 在【登录策略】区域，单击【会话超时时间】模块的编辑按钮，修改会话超时时间。
3. 修改完成后，单击【确定】。

策略管理
相关定义
权限

最近更新时间: 2024-12-19 17:12:00

权限是描述在某些条件下允许或拒绝执行某些操作访问某些资源。

默认情况下，主账号是资源的拥有者，拥有其名下所有资源的访问权限；子账号没有任何资源的访问权限；资源创建者不自动拥有所创建资源的访问权限，需要资源拥有者进行授权。

策略是定义和描述一条或多条权限的语法规范。CAM 支持两种类型的策略，预设策略和自定义策略。预设策略是由云平台创建和管理的一些常见的权限集合，如超级管理员、云资源管理员等，这类策略只读不可写。自定义策略是由用户创建的更精细化的描述对资源管理的权限集合。预设策略不能具体描述某个资源，粒度较粗，而自定义策略可以灵活的满足用户的差异化权限管理需求。

通过给用户或者用户组绑定一个或多个策略完成授权。被授权的策略既可以是预设策略也可以是自定义策略。

策略

最近更新时间: 2024-12-19 17:12:00

策略是用于定义和描述一条或多条权限的语法规范。云的策略类型分为预设策略和自定义策略。CAM 从不同角度切入，为您提供了多种方法来创建和管理策略。若您需要向CAM用户或组添加权限，您可以直接关联预设策略，或创建自定义策略后将自定义策略关联到CAM用户或组。每个策略允许包含多个权限，同时您可以将多个策略附加到一个CAM用户或组。

预设策略

预设策略由云创建和管理，是被用户高频使用的一些常见权限集合，如超级管理员、资源全读写权限等。操作对象范围广，操作粒度粗。预设策略为系统预设，不可被用户编辑。

自定义策略

由用户创建的更精细化的描述对资源管理的权限集合，允许作细粒度的权限划分，可以灵活的满足用户的差异化权限管理需求。例如，为某数据库管理员关联一条策略，使其有权管理云数据库实例，而无权管理云服务器实例。

授权指南
创建自定义策略

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何通过不同的创建方式创建自定义策略，自定义策略允许作细粒度的权限划分，可以灵活满足用户的差异化权限管理需求。

前提条件

已登录访问管理控制台，进入策略管理页面。

操作步骤

按策略生成器创建

按策略生成器创建的策略，通过从策略向导中选择服务和操作，并定义资源，自动生成策略语法，简单灵活，优先推荐使用。

1. 在策略管理页面，单击左上角的【新建自定义策略】。
2. 在弹出的选择创建方式窗口中，单击【按策略生成器创建】，进入选择服务和操作页面。
3. 在选择服务和操作页面，补充以下信息。
   - 服务（必选）：选择需要添加的产品。
   - 操作（必选）：选择您要授权的操作。
   - 资源（必填）：填入您要授权的资源的资源六段式。授权粒度为操作级、服务级的云产品不支持填写具体资源六段式，填「*」即可，授权粒度为资源级的云产品资源描述方式请参阅 支持 CAM 的产品 中对应产品的「访问管理指南」文档。云产品支持的授权粒度请参阅 支持 CAM 的产品 中的「授权粒度」。
   - 条件（选填）：设置子账号上述授权的生效条件。详细可参阅 生效条件。

> 说明
>
> - 一条策略中可以添加多条声明。

4. 单击【添加声明】>【下一步】，进入编辑策略页面。

5. 在策略编辑页面，补充策略名称、描述信息，确认策略内容，其中策略名称和策略内容由控制台自动生成。

> 说明
>
> - 策略名称默认为 "policygen" ，后缀数字根据创建日期生成。您可进行自定义。
> - 策略内容与第 3 步的服务和操作对应，您可根据实际需求进行修改。

6. 单击【完成】，完成按策略生成器创建自定义策略的操作。

按标签授权

按标签授权的策略，将具有一类标签属性的资源快速授权给用户或用户组。

1. 在策略管理页面，单击左上角的【新建自定义策略】。
2. 在弹出的选择创建方式窗口中，单击【按标签授权】，进入按标签授权页面。

- 赋予用户/用户组：勾选需要授权的用户/用户组。（可选其一）
- 在标签键：选择需要授权的标签键。（必填项）
- 且具有标签值：选择需要授权的标签值。（必填项）
- 的资源：默认为管理权限。

4. 在按标签授权页面选择以下信息，单击【下一步】，进入检查页面。
5. 在检查页面，确认策略名称、策略内容后单击【完成】，完成按标签授权创建自定义策略操作。其中默认的策略名称和策略内容由控制台自动生成，策略名称默认为 "policygen"，后缀数字根据创建日期生成。

授权管理

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何通过策略关联用户/用户组/角色和如何通过用户/用户组/角色关联策略。关联成功后，用户/用户组/角色将通过策略获得对应的权限。

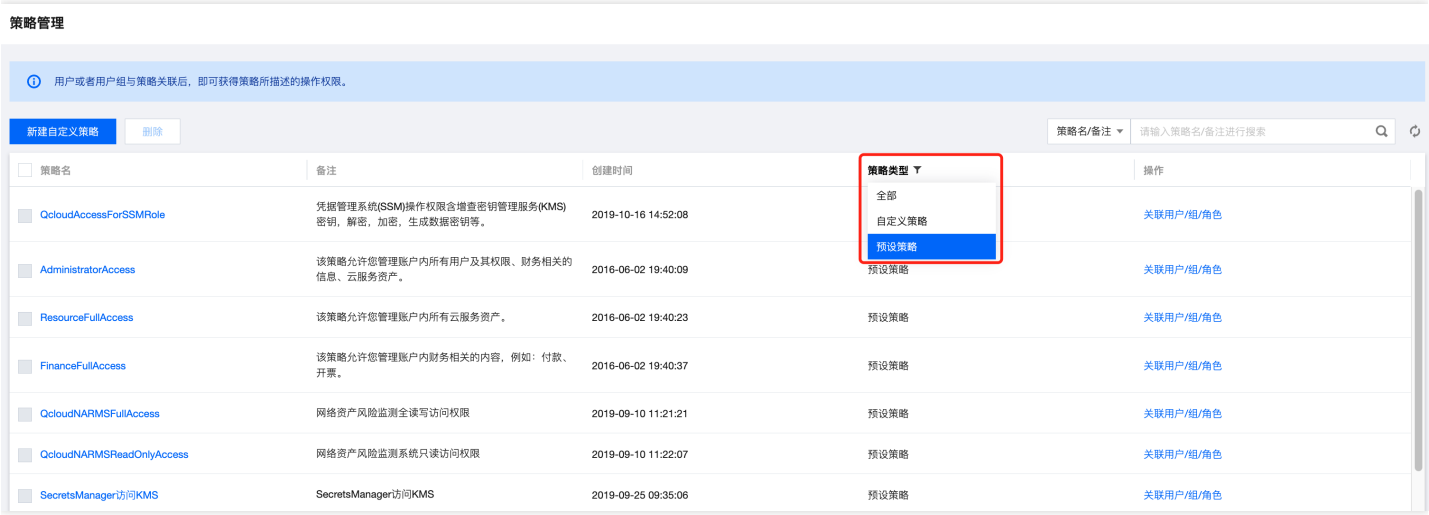
前提条件

已登录 访问管理控制台。

操作步骤

通过策略关联用户/用户组/角色

1. 在访问管理控制台，单击左侧【策略管理】，进入【策略管理】页面。
2. 在【策略管理】页面，根据业务需要在【策略类型】中选择预设策略或自定义策略。



3. 找到需要授权的预设策略，单击右侧【操作】列的【关联用户/组/角色】。
4. 在弹出的【关联用户/组/角色】对话框，根据业务需要在【类型】中选择用户、用户组或角色。



5. 勾选要关联的用户、用户组或角色。
6. 单击【确定】，完成通过策略关联用户操作。

通过用户/用户组关联策略

通过用户关联策略

1. 在访问管理控制台，单击左侧【用户管理】，进入【用户管理】页面。
2. 选择指定用户，单击用户名称，进入【用户详情】页面。
3. 在【已关联的策略】下，单击【关联策略】，打开【关联策略】对话框。
4. 在【关联策略】对话框中，勾选需要授权的策略。
5. 单击【确定】，完成通过用户关联自定义策略操作。

通过用户组关联策略

1. 在访问管理控制台，单击左侧【用户组】，进入【用户管理】页面。
2. 找到需要授权的用户组，单击用户组名称，进入用户组详情页。

3. 在【已关联的策略】下，单击【关联策略】，打开【关联策略】对话框。
4. 在弹出的【关联策略】对话框中，勾选需要授权的策略。
5. 单击【确定】，完成通过用户组关联预设策略操作。

限制IP访问

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何通过自定义策略限制子账号访问 IP，设置成功后，子账号将通过所设置的 IP 管理主账号下的资源，或者拒绝子账号通过设置的 IP 管理主账号下资源。

前提条件

需要设置的产品支持按 IP 限制业务访问，详细可参考 常见问题。

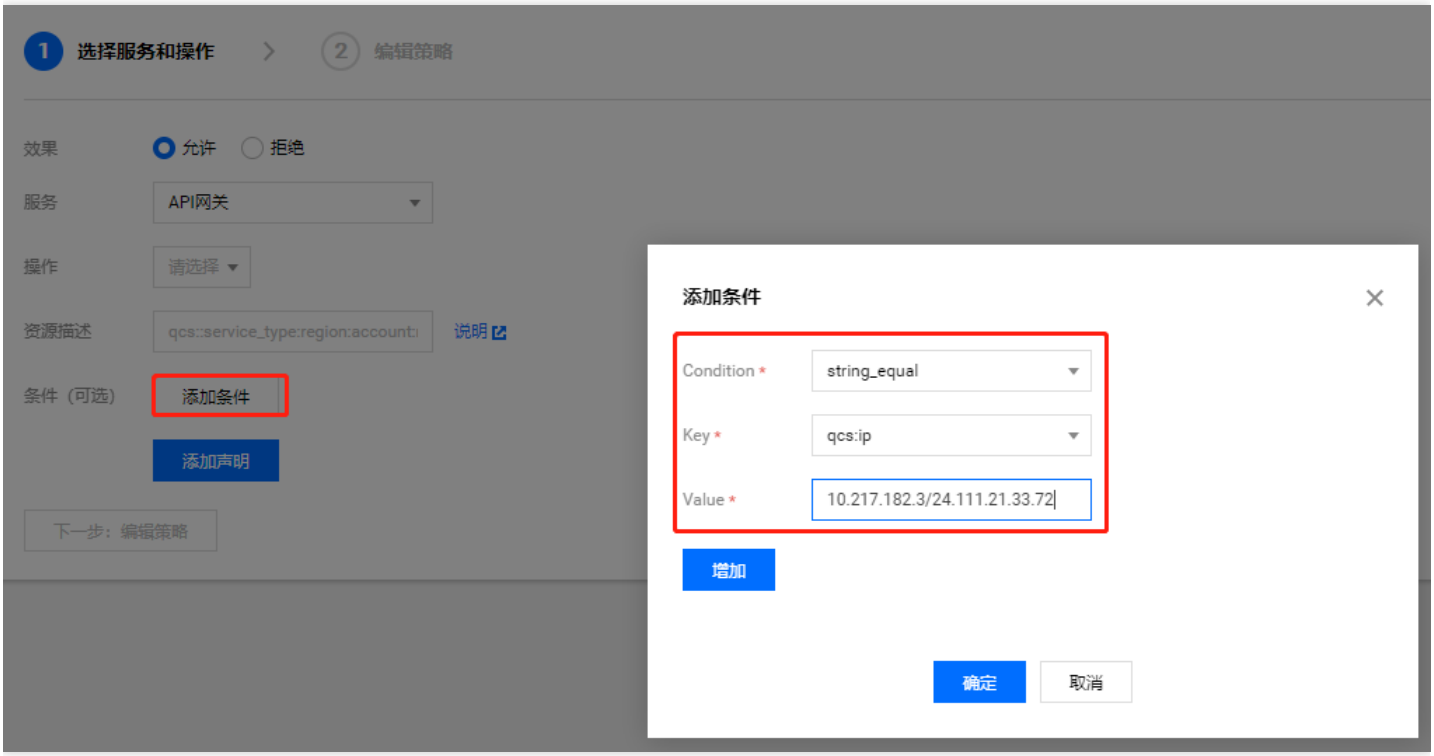
操作步骤

1. 进入 策略管理页面，单击左上角的【新建自定义策略】。
2. 在弹出的选择创建方式窗口中，单击【按策略生成器创建】，进入选择服务和操作页面。
3. 在选择服务和操作页面，补充以下信息。

- 效果：必填项，选择 "允许"。如选择 "拒绝"，用户或用户组不能获取授权。
- 服务：必填项，选择需要添加的产品。
- 操作：必填项，根据您的需求勾选产品权限。
- 资源：必填项，您可以参考 资源描述方式填写。
- 条件：根据您的需求选择条件，输入 IP 地址。可以添加多条限制。例如，效果选择"允许"，仅限使用该 IP 地址的用户或组获取授权。

使用示例

以下示例表示用户必须在 10.217.182.3/24 或者 111.21.33.72/24 网段才能调用云 API 访问 cos:PutObject，如下图：



策略语法如下：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": "cos:PutObject",
"resource": "*",
"condition": {
"ip_equal": {
"qcs:ip": [
"10.217.182.3/24",
"111.21.33.72/24"
]
}
}
}
]
}
```

语法逻辑
元素参考

最近更新时间: 2024-12-19 17:12:00

策略(policy)由若干元素构成，用来描述授权的具体信息。核心元素包括委托人(principal)、操作(action)、资源(resource)、生效条件(condition)以及效力(effect)。元素保留字仅支持小写。它们在描述上没有顺序要求。对于策略没有特定条件约束的情况，condition 元素是可选项。在控制台中不允许写入 principal 元素，仅支持在策略管理 API 中和策略语法相关的参数中使用 principal。

1.版本(version)

描述策略语法版本。该元素是必填项。目前仅允许值为"2.0"。

2.委托人(principal)

描述策略授权的实体。包括用户（开发商、子账号、匿名用户）、用户组，未来会包括角色、联合身份用户等更多实体。仅支持在策略管理API中策略语法相关的参数中使用该元素。

3.语句(statement)

描述一条或多条权限的详细信息。该元素包括 action、resource、condition、effect 等多个其他元素的权限或权限集合。一条策略有且仅有一个statement 元素。

4.操作(action)

描述允许或拒绝的操作。操作可以是 API（以name前缀描述）或者功能集（一组特定的 API，以 permid 前缀描述）。该元素是必填项。

5.资源(resource)

描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。有关如何指定资源的信息，请参阅您编写的资源声明所对应的产品文档。该元素是必填项。

6.生效条件(condition)

描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息。有些服务允许您在条件中指定其他值。该元素是非必填项。

7.效力(effect)

描述声明产生的结果是"允许"还是"显式拒绝"。包括 allow(允许)和deny(显式拒绝)两种情况。该元素是必填项。

8.策略样例

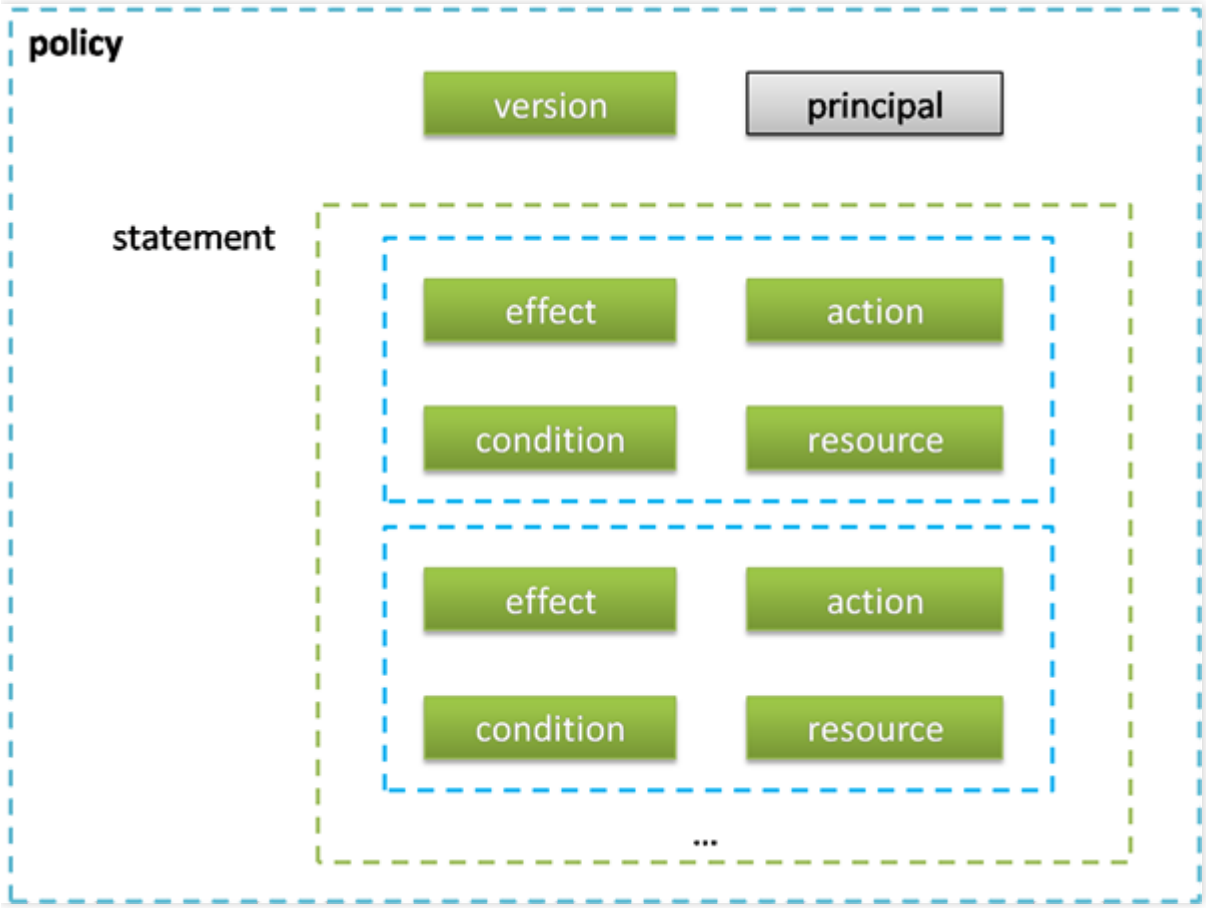
该样例描述为：允许属于开发商 ID 1238423下的子账号 ID 3232523以及组 ID 18825， 对北京地域的cos存储桶 bucketA和广州地域的 cos 存储桶 bucketB 下的对象 object2，在访问 IP 为10.121.2.*网段时，拥有所有 cos 读 API 的权限以及写对象的权限，以及可以发送消息队列的权限。

```
{
"version": "2.0",
"principal": {
"qcs": [
"qcs::cam::uin/1238423:uin/3232523",
"qcs::cam::uin/1238423:groupid/18825"
]
},
"statement": [
{
"effect": "allow",
"action": [
"name/cos:PutObject",
"permid/280655"
],
"resource": [
"qcs::cos:bj:uid/1238423:prefix//1238423/bucketA/*",
"qcs::cos:gz:uid/1238423:prefix//1238423/bucketB/object2"
],
"condition": {
"ip_equal": {
"qcs:ip": "10.121.2.10/24"
}
}
},
{
"effect": "allow",
"action": "name/cmqqueue:Sendmessages",
"resource": "*"
}
]
}
```

语法结构

最近更新时间: 2024-12-19 17:12:00

整个策略的语法结构如下图所示。策略 policy 由版本 version 和语句 statement 构成，还可以包含委托人信息 principal，委托人仅限于策略管理 API 中策略语法相关的参数中使用。 语句 statement 是由若干个子语句构成。每条子语句包括操作 action、资源 resource、生效条件 condition 以及效力 effect 四个元素，其中 condition 是非必填项。



JSON 格式

策略语法以 JSON 格式为基础。创建或更新的策略不满足 JSON 格式时，将无法提交成功，所以用户必须要确保 JSON 格式正确。 JSON 格式标准在 RFC7159 中定义，您也可以使用在线 JSON 验证程序检查策略格式。

语法约定

语法描述中有如下约定：

- 以下字符是包含在策略语法中的 JSON 字符：

```
{ } [ ] " , :
```

- 以下字符是用于描述策略语法中的特殊字符，不包含在策略中：

```
= < > ( ) |
```

- 当一个元素允许多个值时，使用逗号分隔符和省略号进行表示。例如：

```
[<resource_string>, < resource_string>, ...]
<principal_map> = { <principal_map_entry>, > <principal_map_entry>, ... }
```

允许多个值时，也可以只包含一个值。当元素只有一个值时，尾部的逗号必须去掉，且中括号"[]"标记可选。例如：

```
"resource": [<resource_string>]
"resource": <resource_string>
```

- 元素后的问号 (?) 表示该元素是非必填项。例如：

```
<condition_block?>
```

- 元素是枚举值的情况下，枚举值之间用竖线 "|" 表示，并用 "()" 括号定义枚举值的范围。例如：

```
("allow" | "deny")
```

- 字符串元素用双引号包括起来。例如：

```
<version_block> = "version" : "2.0"
```

语法描述

```
policy={
<version_block><principal_block?>,
<statement_block>
}<version_block>="version": "2.0"<statement_block>="statement": [
<statement>,
<statement>,
...
]<statement>={
<effect_block>,
<action_block>,
```

```
<resource_block>,
<condition_block?>
}<effect_block>="effect": ("allow"|"deny")<principal_block>="principal": ("*"|<principal_map>)<princ
ipal_map>={
<principal_map_entry>,
<principal_map_entry>,
...
}<principal_map_entry>="qcs": [
<principal_id_string>,
<principal_id_string>,
...
]<action_block>="action": ("*"|[
<action_string>,
<action_string>,
...
])<resource_block>="resource": ("*"|[
<resource_string>,
<resource_string>,
...
])<condition_block>="condition": {
<condition_map>
}<condition_map>{
<condition_type_string>: {
<condition_key_string>: <condition_value_list>
},
<condition_type_string>: {
<condition_key_string>: <condition_value_list>
},
...
}<condition_value_list>=[
<condition_value>,
<condition_value>,
...
]<condition_value>=("string"|"number")
```

语法说明：

- 一个策略 policy 可以包含多条语句 statement。 策略的最大长度是 4096 个字符（不包含空格），具体信息请参阅 限制。 各个块 block 的显示顺序无限制。例如，在策略中， version_block 可以跟在 effect_block 后面等。
- 当前支持的语法版本为 2.0。
- principal_block 元素在控制台中不允许写入，仅支持在策略管理 API 中和策略语法相关的参数中使用 principal 。

- 操作 action 和资源 resource 都支持列表，其中 action 还支持各产品定义的操作集 permid。
- 生效条件可以是单个条件，或者包括多个子条件块的逻辑组合。每个生效条件包括条件操作符 condition_type、条件键 condition_key，条件值 condition_value。
- 每条语句 statement 的效力 effect 为 deny 或 allow 。当策略中包含的语句中既包含有 allow 又包含有 deny 时，遵循 deny 优先原则。

字符串说明

语法描述的元素字符串说明如下：

action_string

由描述作用域、服务类型和操作名称组成。

```
//所有产品所有操作
"action":"*"
"action":"*:*"
// COS 产品所有操作
"action":"cos:*"
// COS 产品的名为 GetBucketPolicy 的操作
"action":"cos:GetBucketPolicy"
// COS 产品部分匹配 Bucket 的操作
"action":"cos:*Bucket*"
//操作集 ID 为 280649 的操作列表
"action":"permid/280649"
// cos 产品，名为 GetBucketPolicy\PutBucketPolicy\DeleteBucketPolicy 的操作列表
"action":["cos:GetBucketPolicy","cos:PutBucketPolicy","cos: DeleteBucketPolicy"]
```

其中，permid 为各产品定义的操作集合 ID ，具体信息请参阅各相关产品文档。

resource_string

资源通过六段式描述。

```
qcs: project :serviceType:region:account:resource
```

示例如下所示：

```
// COS 产品的 object 资源，上海地域，资源拥有者的 uid 是10001234，资源名是 bucket1/object2 ，资源前缀是 prefix
qcs::cos:sh:uid/10001234:prefix//10001234/bucket1/object2
// CMQ 产品的队列，上海地域，资源拥有者的 uin 是12345678，资源名是12345678/queueName1,资源前缀是 queueName
qcs::cmqqueue:sh:uin/12345678:queueName/12345678/queueName1
```

```
// CVM 产品的云服务器，上海地域，资源拥有者的 uin 是12345678，资源名是 ins-abcdefg,资源前缀是 ins
tance
qcs::cvm:sh:uin/12345678:instance/ins-abcdefg
```

具体信息请参阅各产品的 **支持的资源级权限** 页面的资源描述方法。

condition_type_string

条件操作符，描述测试条件的类型。例如 string_equal、string_not_equal、date_equal、date_not_equal、ip_equal、ip_not_equal、numeric_equal、numeric_not_equal 等。示例如下所示:

```
"condition":{
"string_equal":{"cvm:region":["sh","gz"]},
"ip_equal":{"qcs:ip":"10.131.12.12/24"}
}
```

condition_key_string

条件键，表示将对其值采用条件操作符进行操作，以便确定条件是否满足。CAM 定义了一组在所有产品中都可以使用的条件键，包括 qcs:current_time、qcs:ip 、qcs:uin 和 qcs:owner_uin 等。具体信息请参阅 生效条件。

principal_id_string

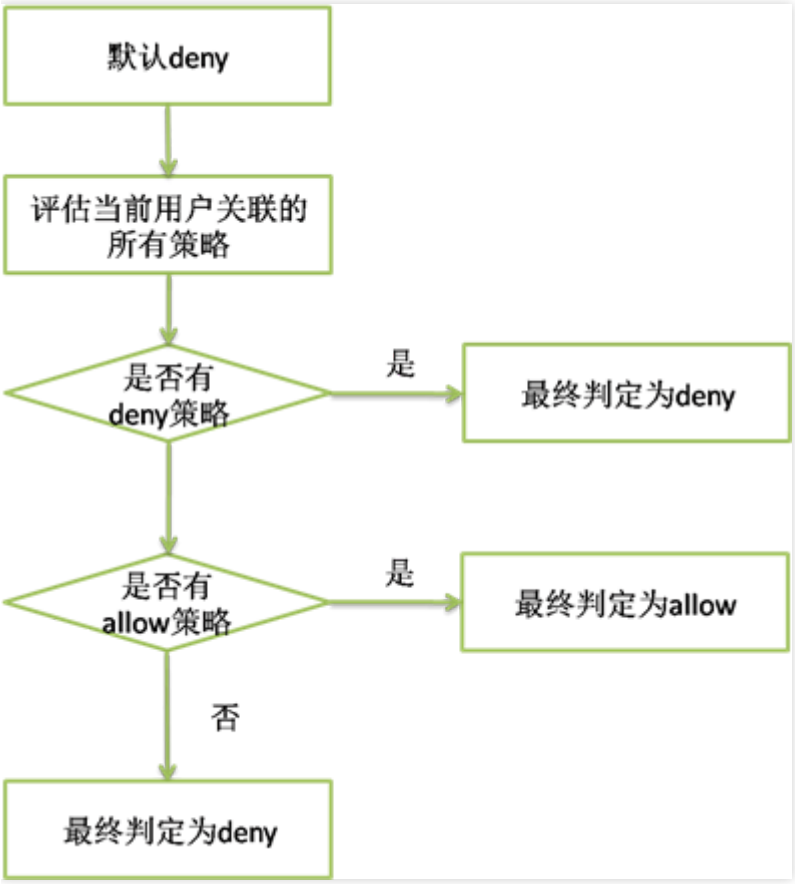
对于 CAM 而言，用户也是它的资源。因此委托人 principal 也采用六段式描述。示例如下，具体信息请参阅 资源描述方式。

```
"principal": {"qcs":["qcs::cam::uin/1238423:uin/3232",
"qcs::cam::uin/1238423:groupid/13"]}
```

评估逻辑

最近更新时间: 2024-12-19 17:12:00

云平台用户访问云资源时， CAM 通过以下评估逻辑决定允许或拒绝。



1. 默认情况下，所有请求都将被拒绝。
2. CAM 会检查当前用户关联的所有策略。
3. 判断是否匹配策略，是则进行下一步判断；否则最终判断为 deny ，不允许访问云资源。
4. 判断是否有匹配 deny 策略，是则最终判定为 deny ，不允许访问云资源；否则进行下一步判断。
5. 判断是否有匹配 allow 策略，是则最终判断为 allow ，允许访问云资源；否则最终判定为 deny，不允许访问云资源。

> **注意：**

- 对于根账号，默认拥有其名下所有资源的访问权限。
- 有些通用策略，会默认关联所有 CAM 用户。具体请见下文的 通用策略表。
- 其他策略都必须显式指定，包括 allow 和 deny 策略。
- 对于支持跨帐号资源访问的业务，存在权限传递的场景，即根账号 A 授权根账号 B 下的某个子账号对其资源的访问权限。这个时候 CAM 会同时校验 A 是否授权给 B 该权限以及 B 是否授权给子帐号该权限，两者同时满足的前提下， B 的子账号才有权访问 A 的资源。

目前支持的通用策略表如下：

策略说明	策略定义

查询密钥需要 MFA 验证	{
	"principal":" ",
	"action":"account:QueryKeyBySecretId",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

设置敏感操作需要 MFA 验证	{
	"principal":" ",
	"action":"account:SetSafeAuthFlag",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

绑定 token 需要 MFA 验证	{
	"principal":" ",
	"action":"account:BindToken",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

解绑 token 需要 MFA 验证	{
	"principal":" ",
	"action":"account:UnbindToken",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

修改邮箱需要 MFA 验证	{
	"principal":" ",
	"action":"account:ModifyMail",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

策略说明	策略定义

修改手机号需要 MFA 验证	{
	"principal":" ",
	"action":"account:ModifyPhoneNum",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

资源描述方式

最近更新时间: 2024-12-19 17:12:00

资源 resource 元素描述一个或多个操作对象，如 CVM 资源、COS存储桶等。本文档主要介绍 CAM 的资源描述信息。

六段式

所有资源均可采用下述的六段式描述方式。每种产品都拥有其各自的资源和对应的资源定义详情。有关如何指定资源的信息，请参阅对应的产品文档。 六段式定义方式如下所示：

```
qcs:project_id:service_type:region:account:resource
```

其中：

- qcs 是 qcloud service 的简称，表示是云平台的云资源。该字段是必填项。
- project_id 描述项目信息，仅兼容 CAM 早期逻辑。当前策略语法禁止填写该信息。
- service_type 描述产品简称，如 CVM、CDN等，产品的检测具体细节请参考对应的产品文档。值为 `*` 的时候表示所有产品。该字段是必填项。
- region 描述地域信息。值为空的时候表示所有地域。云平台新版地域统一命名方式请参考 地域和可用区。云平台现有的地域命名方式定义如下：

地域缩写	描述
gz	广州
sh	上海
shjr	上海金融区
bj	北京
cd	成都

- account 描述资源拥有者的根账号信息。目前支持两种方式描述资源拥有者，uin 和 uid 方式。
- uin 方式，即根账号的 QQ 号，表示为 `uin/${uin}` ，如 uin/12345678；

- uid 方式，即根账号的 APPID，表示为 `uid/${appid}` ，如 uid/10001234。
- 值为空的时候表示创建策略的 CAM 用户所属的根账号。目前COS和CAS业务的资源拥有者只能用uid方式描述（如不涉及，无需关注），其他业务的资源拥有者只能用 uin 方式描述。
- resource 描述各产品的具体资源详情。
    i. 有几种描述方式，该字段是必填项。
    ii. 表示某个资源子类下的资源 ID 。如 VPC 产品的 `instance/ins-abcdefg` 。

```
<resource_type>/<resource_id>
```

2. 表示某个资源子类下的带路径的资源 ID 。如 COS 产品的`prefix//10001234/bucket1/object2`。该方式下，支持目录级的前缀匹配。如`prefix//10001234/bucket1/*`，表示 bucket1 下的所有 Object 。

```
<resource_type>/<resource_path>
```

3. 表示某个资源子类下的所有资源。如 `instance/*`。

```
<resource_type>/*
```

4. 表示某产品下的所有资源。

```
*
```

2. 在某些场景下，资源 resource 元素也可以用 `*` 来描述，含义定义如下，详细信息也请参阅对应的产品文档。
3. 操作 action 是需要关联资源的操作时，resource 定义为 `*` ，表示关联所有资源。
4. 操作 action 是不需要关联资源的操作时，resource 都需要定义为 `*` 。

CAM 的资源定义

CAM 包含了用户、组、策略等资源，CAM 资源的描述方式如下所示：

根账号：

```
qcs::cam::uin/164256472:uin/164256472
```

或

```
qcs::cam::uin/164256472:root
```

子账号：

```
qcs::cam::uin/164256472:uin/73829520
```

组：

```
qcs::cam::uin/164256472:groupid/2340
```

所有用户：

```
qcs::cam::anonymous:anonymous
```

或

```
*
```

策略：

```
qcs::cam:: uin/12345678:policyid/*
```

或

```
qcs::cam:: uin/12345678:policyid/12423
```

资源的重要说明

- 资源的拥有者一定是根账号。如果资源是子账号创建的，不会自动拥有资源的访问权限，需要由资源拥有者授权。
- COS、CAS等业务支持跨账号授权资源的访问权限。被授权账号可以通过权限传递方式将资源授权给其子账号。

策略变量

最近更新时间: 2024-12-19 17:12:00

使用场景

场景假设：您希望给每个 CAM 用户授予其创建资源的访问权限。例如您想要设置 COS 资源的创建者默认拥有该资源的访问权限。 如果由资源拥有者(根账号)将资源逐个授权给资源创建者，授权成本很高，需要为每种资源都编写策略并授权给创建者。在这种情况下，您可以通过使用策略变量来实现您的需求。在策略的资源定义中增加占位符描述的创建人信息，该占位符即使策略变量。当鉴权时，策略变量将被替换为来自请求本身的上下文信息。

授予创建者资源读权限的策略描述方式如下：

```
{
"version":"2.0",
"statement":
{
"effect":"allow",
"action":"name/cos:Read*",
"resource":"qcs::cos::uid/1238423:prefix/${uin}/*"
}
}
```

- 策略变量在每个资源的路径中带上创建人的 uin。如uin 为12356 的用户创建了名为 test 的 bucket，则其对应的资源描述方式为

```
qcs::cos::uid/1238423:prefix/12356/test
```

- uin 为 12356 的用户访问该资源时，鉴权过程中会把对应的策略信息的占位符替换为访问者，即

```
qcs::cos::uid/1238423:prefix/12356/
```

- 策略中的资源 `qcs::cos::uid/1238423:prefix/12356/` 可以通过前缀匹配访问资源 `qcs::cos::uid/1238423:prefix/12356/test` 。

策略变量的位置

资源元素位置 ：策略变量可以用在[资源六段式]的最后一段。 **条件元素位置** ：策略变量可以用在条件值中。

以下策略表示 VPC 创建者拥有访问权限。

```
{
"version":"2.0",
"statement":
{
"effect":"allow",
"action":"name/vpc:*",
"resource":"qcs::vpc::uin/12357:vpc/*"
"condition":{"string_equal":{"qcs:create_uin":"${uin}"}}
}
}
```

策略变量列表

目前支持的策略变量列表如下：

变量名	变量含义
${uin}	当前访问者的子账号 uin 。对于访问者是根账号的情况，它和根账号 uin 一致。
${owner_uin}	当前访问者所属的根账号 uin 。
${app_id}	当前访问者所属的根账号的 APPID 。

生效条件

最近更新时间: 2024-12-19 17:12:00

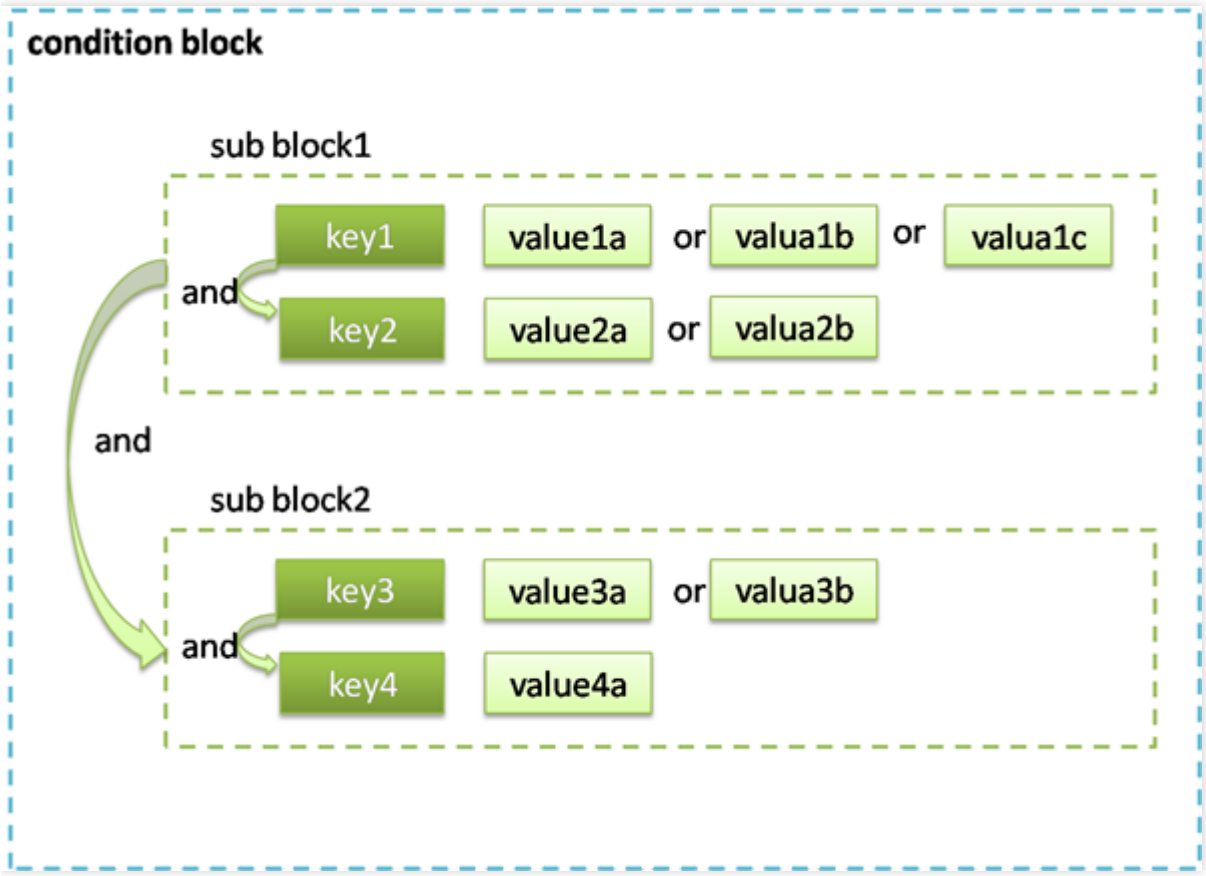
使用场景

在很多场景下，我们需要对创建的策略进一步约束生效的条件 condition 。

- 场景1： CAM 用户调用云 API 时，需要限制用户访问来源，则要求在现有的策略基础上加上 IP 条件。
- 场景2：当 CAM 用户在调用 VPC 对等连接 API 时，除了需要判断 CAM 用户是否拥有对等连接 API 和对等连接资源的访问权限外，还需要确认 CAM 用户是否拥有对等连接关联的 VPC 的访问权限。

语法结构

生效条件的语法结构如下图所示。一个条件块可以由若干个子条件块 sub block 构成，每个子条件块 sub block 对应一个条件操作符和若干个多个条件键，每个条件键对应了若干个条件值。



评估逻辑

条件生效的评估逻辑如下所述：

1. 条件键会对应到多个条件值，只要上下文信息中的对应键值在关联的条件操作符作用下满足其中任意一个条件值，则条件生效。

2. 对于一个子条件块中存在多个条件键的情况下，只有每个条件键对应的条件都生效时，该子条件块才生效。

3. 对于包含多个子条件块的情况，只有每个子条件块都生效时，整个条件才生效。

4. 对于包含 _if_exist 后缀的条件操作符，即使上下文信息中不包含条件操作符所关联的条件键，该条件依然生效。

5. 对于 for_all_value ：限定词约束的条件操作符，适用于上下文信息中的条件键包括多个值的场景。只有当上下文信息中的条件键的每个值在关联的条件操作符作用下生效时，整个条件才生效。

6. 对于 for_any_value ：限定词约束的条件操作符，适用于上下文信息中的条件键包括多个值的场景。只要上下文信息中的条件键的任意一个值在关联的条件操作符作用下生效时，整个条件就可以生效。

使用示例

1. 以下示例表示用户必须在 `10.217.182.3/24` 或者 `111.21.33.72/24` 网段才能调用云 API 。

```
{
"version": "2.0",
"statement": {
"effect": "allow",
"action": "cos:PutObject",
"resource": "*",
"condition": {
"ip_equal": {
"qcs:ip": [
"10.217.182.3/24",
"111.21.33.72/24"
]
}
}
}
}
```

2. 以下示例描述允许 VPC 绑定指定的 NAT 网关， VPC 的地域必须是上海。

```
{
"version": "2.0",
"statement": {
```

```
"effect": "allow",
"action": "name/vpc:AcceptVpcPeeringConnection",
"resource": "qcs::vpc:sh::pcx/2341",
"condition": {
"string_equal_if_exist": {
"vpc:region": "sh"
}
}
}
}
```

条件操作符列表

下表是条件操作符、条件名以及示例的信息。每个产品自定义的条件键，请参阅对应的产品文档。

条件操作符	含义	条件名	举例
string_equal	字符串等于(区分大小写)	qcs:tag	{"string_equal": {"qcs:tag/tag_name1":"tag_value1"}}
string_not_equal	字符串不等于(区分大小写)	qcs:tag	{"string_not_equal": {"qcs:tag/tag_name1":"tag_value1"}}
string_equal_ignore_case	字符串等于(不区分大小写)	qcs:tag	{"string_equal_ignore_case": {"qcs:tag/tag_name1":"tag_value1"}}
string_not_equal_ignore_case	字符串不等于(不区分大小写)	qcs:tag	{"string_not_equal_ignore_case": {"qcs:tag/tag_name1":"tag_value1"}}
string_like	字符串匹配(区分大小写)	qcs:tag	{"string_like": {"qcs:tag/tag_name1":"tag_value1"}}
string_not_like	字符串不匹配等于(区分大小写)	qcs:tag	{"string_not_like": {"qcs:tag/tag_name1":"tag_value1"}}

条件操作符	含义	条件名	举例
date_not_equal	时间不等于	qcs:current_time	{"date_not_equal":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_greater_than	时间大于	qcs:current_time	{" date_greater_than ":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_greater_than_equal	时间大于等于	qcs:current_time	{" date_greater_than_equal ":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_less_than	时间小于	qcs:current_time	{" date_less_than ":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_less_than_equal	时间小于等于	qcs:current_time	{" date_less_than ":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_less_than_equal	时间小于等于	qcs:current_time	{"date_less_than_equal ":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
ip_equal	ip等于	qcs:ip	{"ip_equal":{"qcs:ip ":"10.121.2.10/24"}}
ip_not_equal	ip不等于	qcs:ip	{"ip_not_equal":{"qcs:ip ":["10.121.2.10/24", "10.121.2.20/24"]}}
numeric_not_equal	数值不等于	qcs:mfa	{" numeric_not_equal":{"mfa":1}}
numeric_greater_than	数值大于		{"numeric_greater_than ":{"cvm_system_disk_size":10}}
numeric_greater_than_equal	数值大于等于		{"numeric_greater_than_equal ":{"cvm_system_disk_size":10}}
numeric_less_than	数值小于		{"numeric_less_than ":{"cvm_system_disk_size":10}}
numeric_less_than_equal	数值小于等于		{"numeric_less_than_equal ":{"cvm_system_disk_size":10}}

版权所有：亿算云平台

条件操作符	含义	条件名	举例
numeric_equal	数值等于	qcs:mfa	{" numeric_equal":{"mfa":1}}
numeric_greater_than	数值大于		{"numeric_greater_than ": {"some_key":11}}
bool_equal	布尔值匹配	-	-
null_equal	条件键为空匹配	-	-

说明：

1. 日期格式按照 ISO8601 标准表示，并需要使用 UTC 时间。
2. IP 格式要符合 CIDR 规范。
3. 条件操作符（null_equal除外）加上后缀 _if_exist，表示上下文信息中即便不包含对应的键值依然生效。
4. for_all_value ：限定词搭配条件操作符使用，表示上下文信息中条件键的每个值都满足要求时才生效。
5. for_any_value ：限定词搭配条件操作符使用，表示上下文信息中条件键的任意一个值满足要求时就可以生效。
6. 部分业务不支持条件，或仅支持部分条件。具体信息参考业务文档说明。

角色管理
角色概述

最近更新时间: 2024-12-19 17:12:00

什么是角色

角色可以看作是亿算云平台的“虚拟账号”，角色同样可被授予策略，拥有在亿算云平台中允许执行和拒绝执行的权限。角色可以是任一亿算云平台账号代入，并不是唯一地与某个账号绑定关联。角色没有关联的持久证书（密码或访问密钥），主账号仅在申请角色时需要使用持久证书，在用户担任某个角色时，则会动态创建临时证书并为用户进行相应访问时提供该临时证书，即可通过临时密钥签名调用基础服务的开放 API 来访问用户的云资源。

角色使用场景

云账号角色

云账号角色用于实现跨租户的资源访问。如一些代运维场景，租户A可通过角色来实现让租户B来访问A租户下特定的资源

基本概念

最近更新时间: 2024-12-19 17:12:00

在您开始使用角色前需要了解一些基本术语，包括角色、服务角色、自定义角色、权限策略等。

角色

拥有一组权限的虚拟身份。用于对角色载体授予亿算云平台中服务、操作和资源的访问权限。这些权限附加到角色，而不附加到具体的用户或者用户组。

CAM 支持以下 2 种类型的角色：

- 服务（预设）角色：由服务进行预定义的角色，服务角色需经过用户授权，服务即可通过扮演服务角色对用户资源进行访问操作。
- 自定义角色：由用户自行定义的角色，用户可以自由灵活地决定角色载体和角色权限。

角色可由以下用户使用：

- 可作为角色的主账号。
- 可作为角色的子用户以及协作者。

服务角色

服务角色是各个产品服务直接提供的独特类型的 CAM 预设角色。服务角色的关联权限由相关产品服务预定义，一旦相关产品服务被您赋予服务角色，即该产品服务能够全权代表您调用服务角色权限范围内的其他产品服务。服务角色可以让您更轻松地使用服务，因为在赋予角色的流程中您不必手动添加权限，只需要选择是否给该服务授予服务角色的相关权限。

给相关产品服务赋予服务角色的流程中，服务角色的相关权限和角色载体已经被定义，除非另外定义，否则仅该服务可以代入角色。服务角色的预定义包括角色名称、角色载体、权限策略。

云账号角色

云账号角色是用户自己对 CAM 角色进行定义。自定义角色的角色名称、角色载体以及角色权限均由用户决定。自定义角色可以让您更自由灵活地对您云上资源的访问使用权限进行分配，角色载体为其他租户的主账号

被您授予角色的对象仅在使用角色的过程中能够获得相关权限，避免给予持久密钥可能带来的安全问题。

权限策略

JSON 格式的权限文档。您可以在权限策略中定义角色可使用的操作和资源。该文档规则依赖于 CAM 策略语言规则。

信任策略

JSON 格式的权限文档。您可以在信任策略中定义可扮演角色的对象以及扮演角色时需满足的条件。该文档规则依赖于 CAM 策略语言规则。

创建角色

最近更新时间: 2024-12-19 17:12:00

操作场景

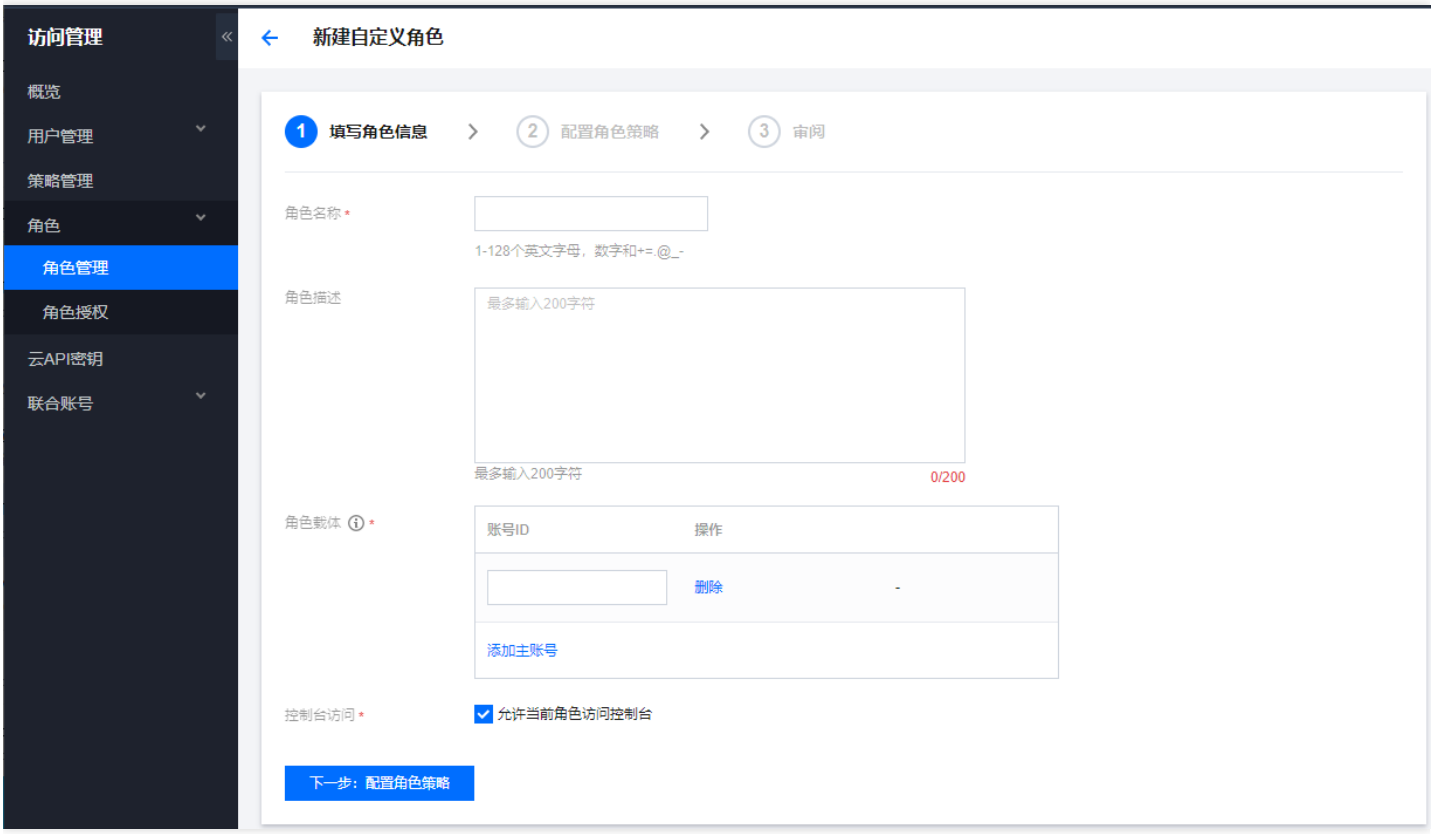
本文档介绍如何创建角色。创建成功后，角色可以在获得的权限范围内管理主账号下的资源。

前提条件

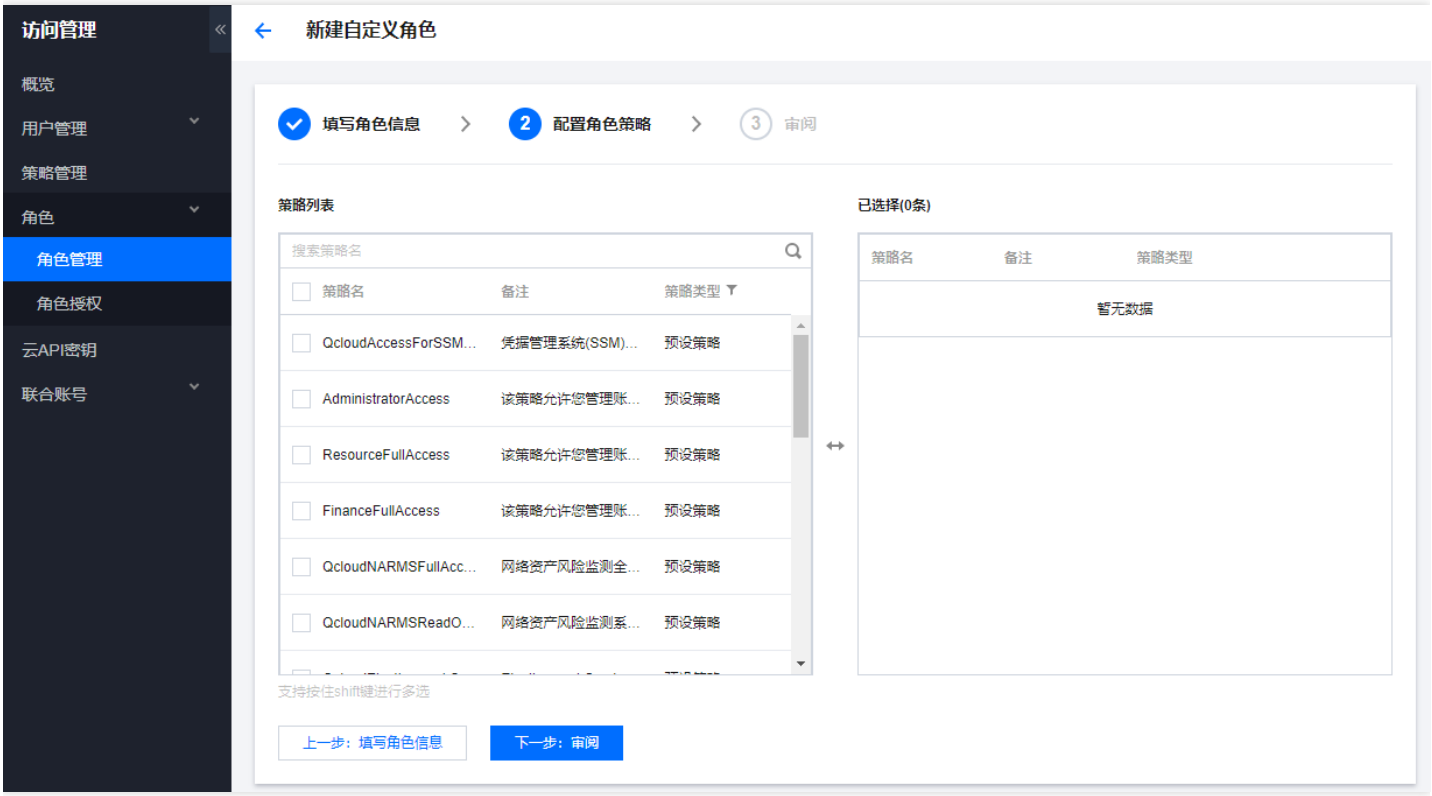
已登录访问管理控制台，进入 角色 列表页面。

操作步骤

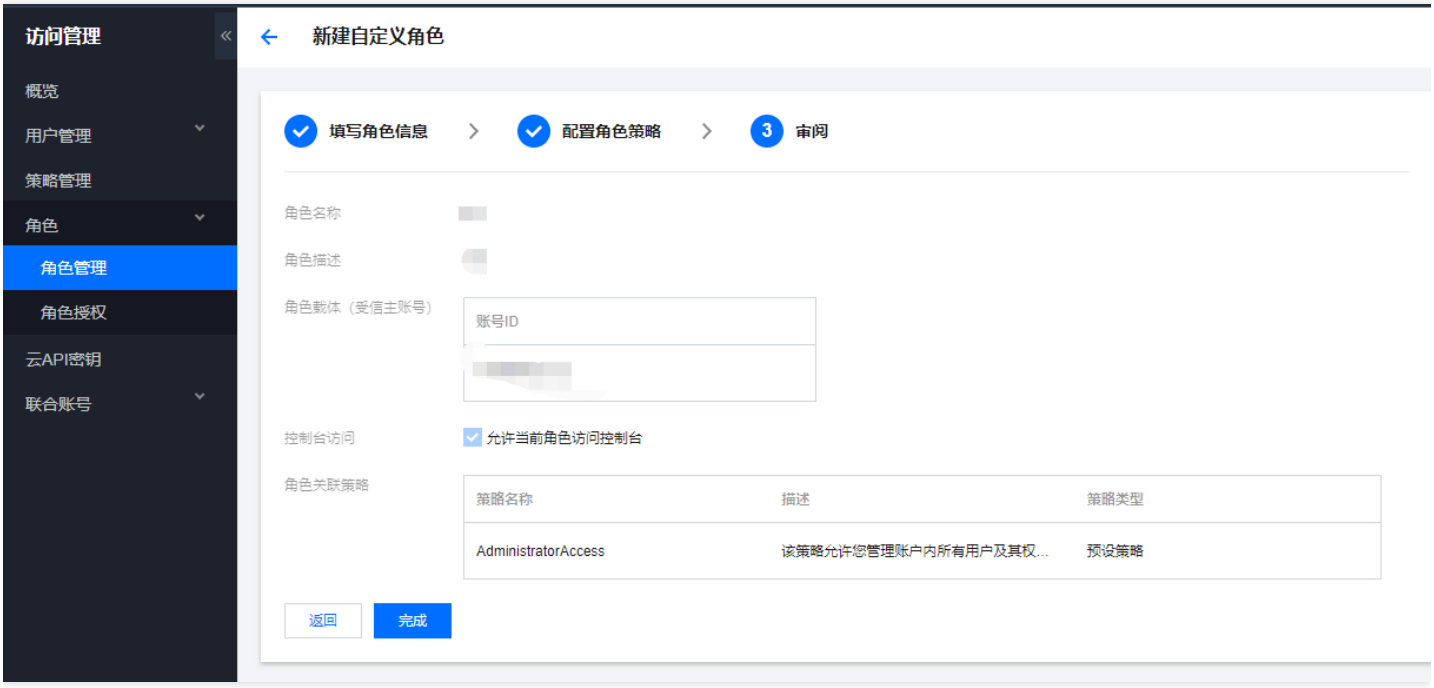
1. 在【访问管理】-【角色】-【角色管理】页面，单击【新建角色】，根据界面提示输入相应参数，单击【下一步：配置角色策略】。



2. 在【策略列表】内勾选您想要给当前角色添加的策略，单击【下一步：审阅】。



3. 对角色相关信息做确认后，单击【完成】。



修改角色

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何修改角色关联策略。修改成功后，角色将根据当前设置在获得的权限范围内管理主账号下的资源。

前提条件

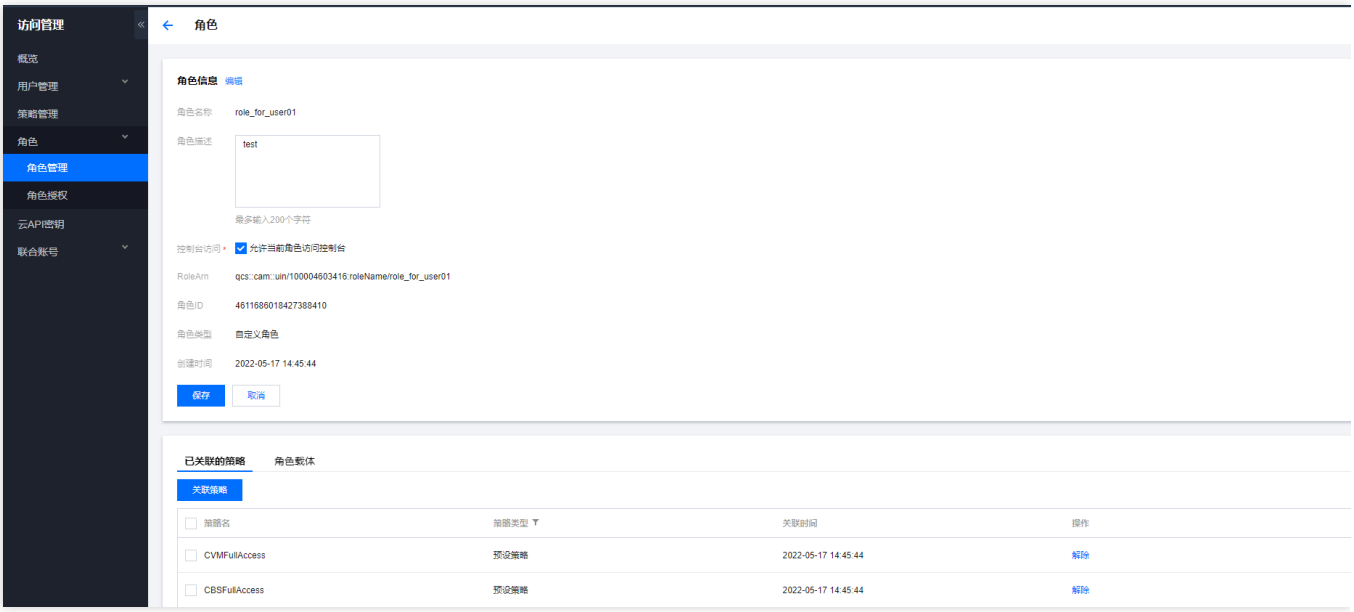
已登录访问管理控制台，进入 角色 列表页面。

操作步骤

修改角色描述

1. 在【角色管理】页面，单击待修改的角色名称，进入角色详情页。

2. 在【角色信息】区域，单击 ，编辑角色描述信息。



3. 单击【保存】，更新角色描述信息。

修改已关联策略

1. 在【角色管理】页面，单击待修改的角色名称，进入角色详情页。
2. 在【已关联的策略】页签，单击【关联策略】。

3. 在弹出的【关联策略】对话框，勾选想要给当前角色添加的策略，单击【确定】，添加角色关联策略。

解决已关联策略

1. 在【角色管理】页面，单击待修改的角色名称，进入角色详情页。
2. 在【已关联的策略】页签，单击待解除策略名对应【操作】列的【解除】。
3. 在弹出的【解除策略】对话框，单击【确认解除】，该角色将无法获得该策略所描述的相关权限。

删除角色

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何删除角色。角色删除后，将无法获取相关权限管理账号下的资源。

操作步骤

1. 登录访问管理（CAM）控制台，进入【角色管理】页面。

2. 单击待删除的角色名对应【操作】列的【删除】。



3. 在弹出的【删除角色】对话框中，单击【确定】，删除该角色，同时解除该服务角色已关联的策略及授权关系。

授权角色

最近更新时间: 2024-12-19 17:12:00

1、在【访问管理】-【角色】-【角色授权】列表里，会列出当前租户可扮演的所有角色列表

2、管理员在操作列点授权扮演，可指定当前租户下，哪些子用户可以通过扮演指定角色来访问对应租户下的资源

3、被授权扮演之后的子用户，在登录控制台后，可以切换角色

4、点击切换角色之后，可以在页面选择要切换的角色名，这里只会列出该子用户有权限的角色列表

为子账号赋予扮演角色策略

最近更新时间: 2024-12-19 17:12:00

作为角色载体的主账号可以允许其子账号对角色进行扮演，这里我们通过一个案例让您轻松了解如何为子账号创建并赋予扮演角色的策略。

假设如下场景，公司 A 有一个运维工程师的职位，并且希望将该职位外包给公司 B，该职位需要操作公司 A 广州地域所有云服务器资源。

公司 A 企业账号 CompanyExampleA（主账号 ID 为 12345），创建一个角色并将角色载体设置为公司 B 的企业账号 CompanyExampleB（主账号 ID 为 67890）。公司 A（CompanyExampleA）调用 CreateRole 接口创建一个角色名称（roleName）为 DevOpsRole 的角色，公司 A 企业账号 CompanyExampleA 为创建的角色 DevOpsRole 附加了权限。

1. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345） 调用 CreateRole 接口创建一个 roleName 为 DevOpsRole 的角色，policyDocument（角色信任策略）参数设为

```
{
"version": "2.0",
"statement": [
{
"action": "name/sts:AssumeRole",
"effect": "allow",
"principal": {
"qcs": ["qcs::cam::uin/67890:root"]
}
}
]
}
```

2. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345） 需要为刚才创建的角色附加权限。

    i. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345） 创建策略 DevOpsPolicy，策略语法如下：

```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": "cvm:*",
"resource": "qcs::cvm:ap-guangzhou::*"
}
```

```
]
}
```

2.公司 A 企业账号 CompanyExampleA（ownerUin 为 12345）调用 AttachRolePolicy 将 step1 中创建的策略绑定到角色 DevOpsRole，入参 policyName=DevOpsPolicy，roleName=DevOpsRole。

3. 经过上面的步骤，公司 A 企业账号 CompanyExampleA（ownerUin 为 12345）完成了角色的创建和授权。

公司 B 企业账号（CompanyExampleB）被授权这个角色后，希望由子账号 DevB 来完成这项工作。公司 B（CompanyExampleB）需要授权子账号 DevB 可以申请扮演公司 A（CompanyExampleA）的角色 DevOpsRole：

1. 创建策略 AssumeRole，示例如下：

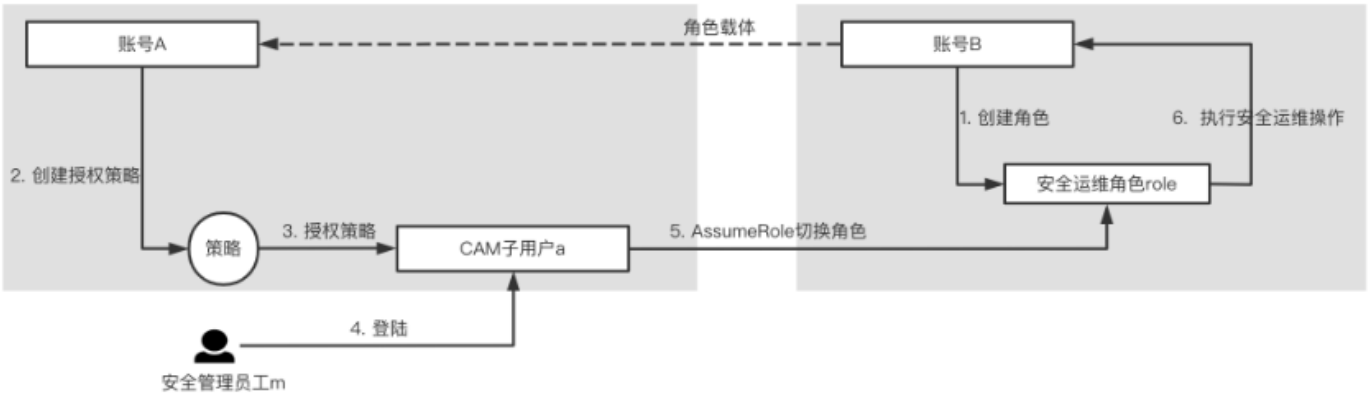
```
{
"version": "2.0",
"statement": [
{
"effect": "allow",
"action": ["name/sts:AssumeRole"],
"resource": ["qcs::cam::uin/12345:roleName/DevOpsRole"]
}
]
}
```

2. 将该策略授权给子账号 DevB。子账号即被赋予了扮演角色 DevOpsRole 的权限。

最佳实践

最近更新时间: 2024-12-19 17:12:00

在创建角色时，可以选择以主账号作为角色载体、创建角色，并为角色绑定授权策略。 作为载体的主账号可以通过创建权限策略，将扮演角色的权限授予其 CAM 子账号，之后 CAM 子账号可以在控制台通过切换角色登录到对应的主账号控制台执行授权范围内的操作，也可以通过云 API 发起跨账号请求。



操作场景

假设企业内有账号 A 和账号 B 两个主账号，企业安全管理员工 m 在账号 A 下有 CAM 子用户 a，员工 m 希望使用该子账号能够同时运维管理账号 B 下的安全信息。这时我们可以按照以下步骤执行操作：

1、在账号 B 下创建安全运维角色 role，并将角色载体指定为主账号 A。

2、在账号 A 下创建权限策略，策略定义了安全运维所需要的一下操作，并将策略关联给角色安全运维角色 role。

3、A的管理员登录平台，在访问管理的角色列表里，授权允许m扮演角色role。

4、员工 m 登录 CAM 子用户 a。

5、员工 m 在控制台选择切换角色，使用安全角色 role 登录控制台。

6、执行安全运维相关操作。

7、如果员工 m 需要同时对多个主账号执行安全运维的相关操作，则可以参照上述步骤为员工 m 授予对应主账号的安全运维权限。

访问密钥
查看当前用户访问密钥

最近更新时间: 2024-12-19 17:12:00

操作场景

本文档介绍如何查看当前登录用户的 API 密钥信息。

前提条件

已登录访问管理控制台，进入 云API 密钥管理 页面。

操作步骤

主账号或子账号可以查看和复制当前账号 API 密钥的 SecretId 和 SecretKey 信息，通过 SecretId 和 SecretKey 在权限范围内使用 API、SDK 或其他开发工具管理主账号下的资源。

1. 进入 API 密钥管理页面，在密钥对列可直接获取复制 SecretId。
2. 在密钥对列，单击【显示】，完成身份验证，可以获取复制SecretKey。

> **说明：**
>
> 如您的子账号需要自助管理 API 密钥，请授予您的子账号 CamFullAccess 策略 权限。

排除故障
如何根据故障反馈创建策略

最近更新时间: 2024-12-19 17:12:00

如何根据故障反馈创建策略

操作场景

本文档介绍如何通过故障反馈创建策略解除故障，解除之后子账号将在新设置的权限范围内管理主账号下的资源。

示例

当拥有 QcloudCVMReadOnlyAccess 策略的子账号尝试进行重装云服务器时将进行如下报错：



如您愿意授权子账号继续进行操作，您可以根据当前报错信息为其创建并关联一个自定义策略。

操作步骤

1. 进入 访问管理 的 策略-控制台，单击新建自定义策略。
2. 在弹出的选择创建方式窗口中，单击【按策略生成器创建】，进入选择服务和操作页面。
3. 在选择服务和操作页面，补充以下信息，如下图所示：



- 效果（必选）：根据授权效果，选择允许还是拒绝。在本次示例中，选择「允许」。
- 服务（必选）：根据产品英文简称选择您要授权的产品。在本次示例中，对应报错信息的 operation 中的「cvm」，您将从产品列表里选择「云服务器」。
- 操作（必选）：选择您要授权的操作。在本次示例中，对应报错信息 operation 中的「ResetInstance」。
- 资源（必填）：填入您要授权的资源的资源六段式。在本次示例中，对应报错信息的「resource」，您可直接复制「qcs:id/1158313:cvm:ap-guangzhou:uin/2159973417:instance/instance/ins-esuithv2」填入。
- 条件（选填）：设置子账号上述授权的生效条件，例如指定 IP 才可访问。在本次示例中，不需要填入。

4. 单击【添加声明】>【下一步】，进入编辑策略页面。
5. 在策略编辑页面，补充策略名称、策略备注信息，确认策略内容，其中策略名称和策略内容由控制台自动生成。

- 策略名称默认为 "policygen" ，后缀数字根据创建日期生成。您可进行自定义。
- 策略内容与步骤 3 的服务和操作对应，您可根据实际需求进行修改。

6. 单击【创建策略】，完成按策略生成器创建自定义策略的操作。
7. 为子账号授权，授权成功后，子账号将获得相应的权限，解除故障。

手机收不到验证信息

现象描述

在进行绑定或者修改手机号码、重置密码等操作时，手机收不到验证信息。

可能原因

导致手机收不到验证信息的主要原因包括：

- 手机号码、区号填写错误。
- 手机系统根据关键词，自动隐藏了内容。
- 手机号码自身原因导致的接收异常，如欠费、网络故障等。

处理步骤

1. 请确认手机号码是否填写正确。

- 是，请执行下一步。
- 否，请 修改手机号码。

2. 请核实手机是否已停机。

- 是，请进行缴费或者更换手机号码。
- 否，请执行下一步。

3. 请确认验证信息是否被视作垃圾短信而被拦截。

- 是，请解除应用软件的短信拦截。
- 否，请执行下一步。

4. 网络通讯异常可能会造成短信丢失，请确认网络通讯是否存在异常。

邮箱收不到验证信息

现象描述

在进行绑定或者修改邮箱、重置密码等操作时，邮箱收不到验证信息。

可能原因

导致邮箱收不到验证信息的主要原因包括：

- 邮箱地址填写错误。
- 邮箱系统根据关键词，自动隐藏了内容。
- 邮箱系统存在特殊限制，导致接收失败。例如，企业的自建邮箱禁止接收第三方邮件。

处理步骤

1. 请确认邮箱地址是否填写正确。

- 是，请执行下一步。
- 否，请 修改邮箱地址。

2. 请确认验证信息是否被视作垃圾邮件，存放在垃圾箱中。

- 是，请将云的邮箱设置为白名单。
- 否，请执行下一步。

3. 网络通讯异常可能会造成邮件丢失，请确认网络通讯是否存在异常。

- 是，请重新获取或稍后再试。
- 否，请执行下一步。

4. 请确认邮箱地址是否为企业自建邮箱，且设置了禁止接收第三方邮件。

企业认证登录管理

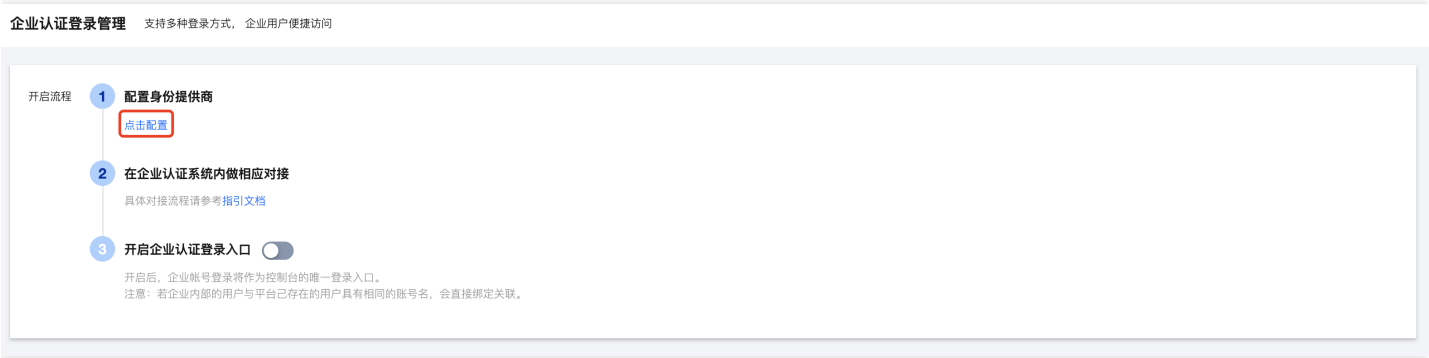
最近更新时间: 2024-12-19 17:12:00

接入准备

- 企业方需要依据认证类型提供相关服务器
- 云平台的容器网络需要可访问企业服务器所在网络，如果网络未配置好，请不要开启企业账号登录，否则导致无法登录租户端 。

接入CAS

1. 进入亿算云平台租户端控制台 ，点击【访问管理】>【企业认证登录管理界面】 页面。



2. 配置企业用户认证CAS相关信息。



- 用户信息字段匹配的意义说明：

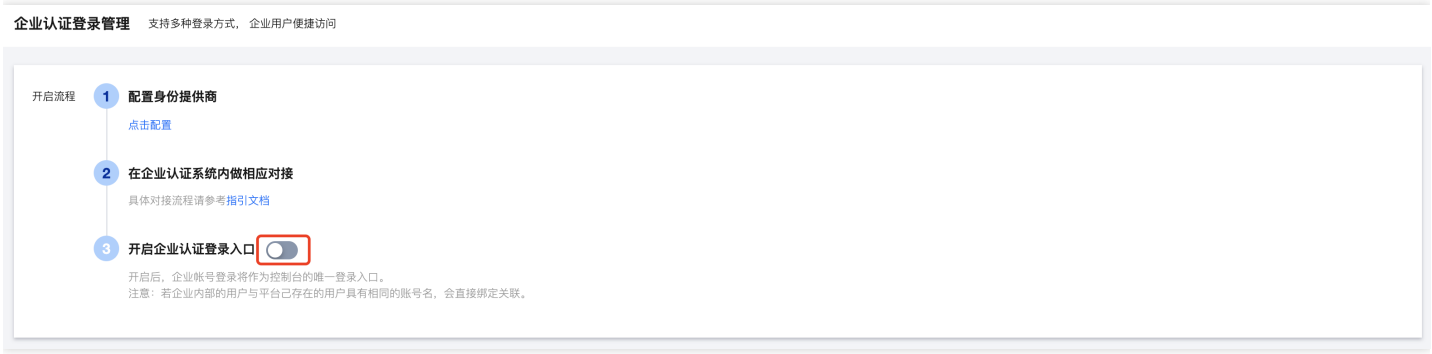
  CAS server端需通过CAS校验ticket url将账号server端的用户信息传给平台，用户信息包括用户名、用户昵称、手机号码和邮箱。对于同样的信息，不同server返回的字段名可能不一样，接入方可在用户信息字段匹配这里对字段名做转换，其中，json里的key表示平台读取的字段，value表示server端返回的字段名，举个例子，若server端返回的用户信息里，用户名字段命名的是user，则value里直接填value，若取的字段名是userName，则value里填写userName

- 账号同步字段意义说明：

  server端需将用户信息传给平台，平台取server端传过来的用户名之后，会检测当前租户下，是否有同名子用户，若平台存在同名子用户，则直接以该子用户身份登录到平台，若当前租户下不存在同名子用户，则会判断账号同步开关是否开启，若账号同步开关开启，则平台会在当前租户下自动创建一个同名子用户，若账号同步开关关闭，则平台会提示，平台不存在子用户，需联系管理员创建



3. 配置企业 CAS 登录、校验地址（以上url网络必须与亿算云平台网络可达），相关地址含义具体可以参考CAS协议说明。
4. 开启企业用户认证。



5. CAS校验 ticket url 需返回 xml cas:serviceResponse ，需包含用户名称、昵称、手机、邮箱，否则无法接入成功！

   其中用户名称、昵称、手机、邮箱字段名称客户可自定义，可在用户信息字段匹配里做映射（参考步骤2）

参数名称	类型	是否必选	描述
cas:user_id	String	是	企业用户登录名称，1-50个英文字母、数字，支持_-.，不支持空格
cas:user_name	String	是	企业用户昵称

参数名称	类型	是否必选	描述
cas:email	String	是	邮箱，必须符合邮箱格式规范
cas:phone	Int	否	手机号码
cas:country_code	String	否	手机号码地区号，如中国：86

企业方 CAS ticket 校验 serviceValidate

响应 xml 格式示例：

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
<cas:authenticationSuccess>
<cas:user>chopin1</cas:user>
<cas:attributes>
<cas:user_id>chopin1</cas:user_id>
<cas:user_name>chopin1</cas:user_name>
<cas:email>chopin1@qq.com</cas:email>
<cas:phone>13999999999</cas:phonel>
<cas:country_code>86</cas:country_code>
</cas:attributes>
</cas:authenticationSuccess>
</cas:serviceResponse>
```

6. 网络层通信验证和配置

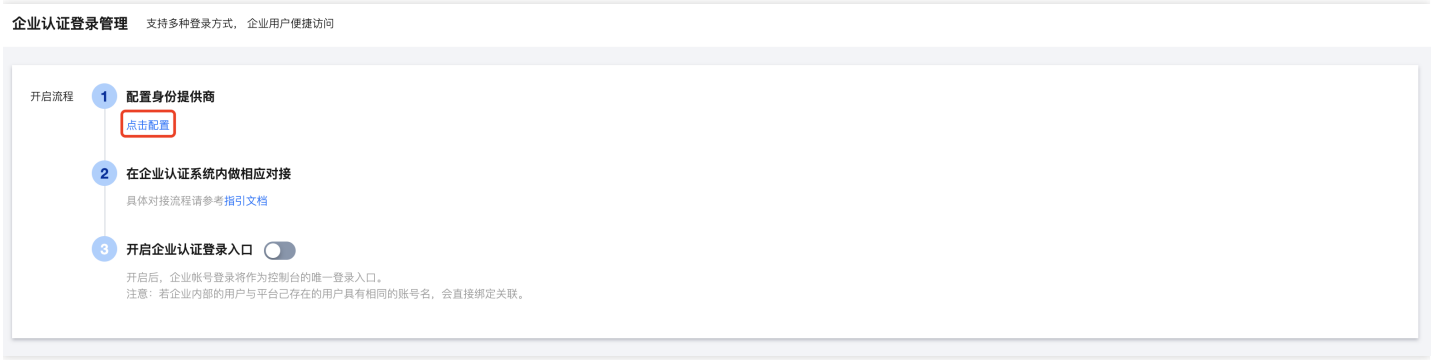
- 进入到亿算云平台集群master节点，进入到 ocloud-tcenter-mc-idplogin pod容器 shell 终端执行：
  i. 验证pod通往企业cas server网络是否可达，注：以下 url 需要填写企业自身 cas server validate 地址
  ii. `curl -v http://cas.gsesgpucloud.com/cas/serviceValidte`
- 验证上述步骤网络是否可达，如果可达，以上步骤配置完成。
- 如果不可达，验证 ocloud-tcenter-mc-idplogin pod 容器是否可以外网或者是否可访问企业cas server网络，网络上可达域名上不可达，则在kube-dns配置上访问的域名，如果网络不可达则联系部署交付实施配置网络与企业网络能正常连通。

7. 配置并开启之后，用户在租户端登录时，需输入主账号ID，目前企业认证登录信息是租户粒度的配置，即每个租户可配置自己的账号server，所以需先输入主账号ID，平台根据主账号ID查询对应的server信息；输入正确的主账号ID之后，平台会自动重定向到企业cas server端，若用户在cas server端是已登录状态，则直接以登录态进入控制台；若用户在cas server端是非登录态，则平台会打开cas server端登录页，用户需在cas server端的登录页输入账号密码在server端登录之后，再以登录态进入控制台



接入OAuth

1. 进入亿算云平台租户端控制台 ，点击【访问管理】>【企业认证登录管理界面】 页面。



2. 配置企业用户认证OAuth相关信息。



3. 配置企业OAuth备注、ClientId、ClientSecret、Oauth验证授权信息url、获取access_token url、获取用户信息url、账号同步开关已经用户信息字段匹配

- 用户信息字段匹配的意义说明：

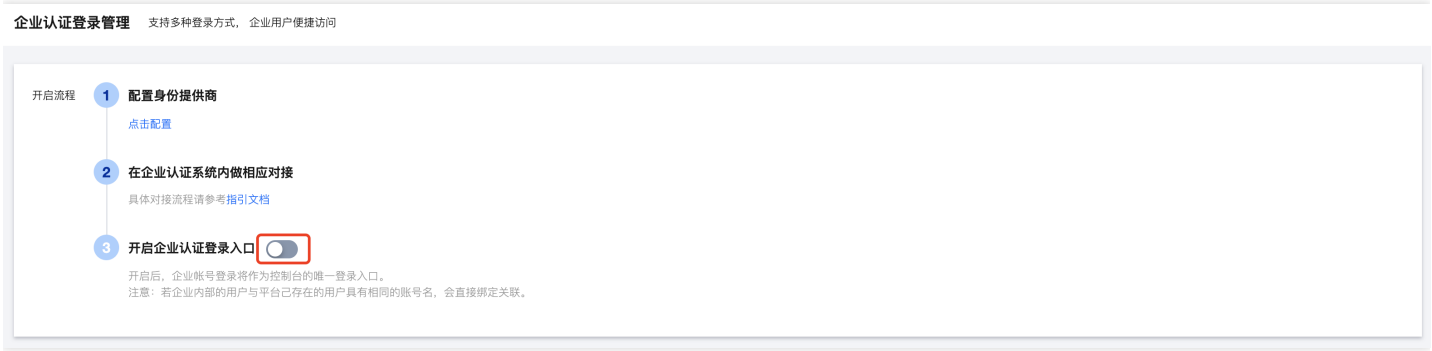
  Oauth server端需通过获取用户信息url将账号server端的用户信息传给平台，用户信息包括用户名、用户昵称、手机号码和邮箱。对于同样的信息，不同server返回的字段名可能不一样，接入方可在用户信息字段匹配这里对字段名做转换，其中，json里的key表示平台读取的字段，value表示server端返回的字段名，举个例子，若server端返回的用户信息里，用户名字段命名的是user，则value里直接填value，若取的字段名是userName，则value里填写userName

- 账号同步字段意义说明：

server端需将用户信息传给平台，平台取server端传过来的用户名之后，会检测当前租户下，是否有同名子用户，若平台存在同名子用户，则直接以该子用户身份登录到平台，若当前租户下不存在同名子用户，则会判断账号同步开关是否开启，若账号同步开关开启，则平台会在当前租户下自动创建一个同名子用户，若账号同步开关关闭，则平台会提示，平台不存在子用户，需联系管理员创建（如下图所示）



4. 开启企业用户认证。



5. 网络层通信验证和配置

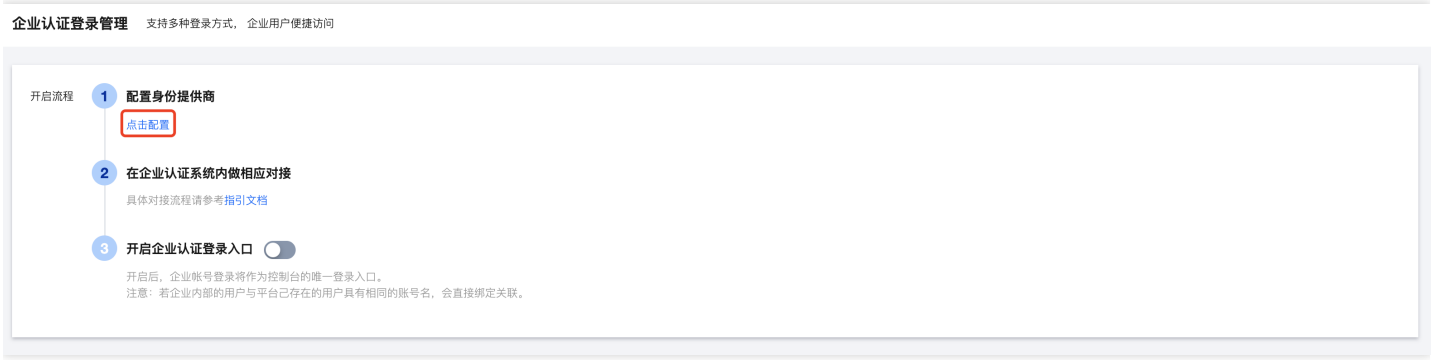
- 进入到亿算云平台集群master节点，进入到 ocloud-tcenter-mc-idplogin pod容器 shell 终端执行：
  i. 验证pod通往企业cas server网络是否可达，注：以下 url 需要填写企业自身 cas server validate 地址
  ii. `curl -v http://cas.gsesgpucloud.com/cas/serviceValidte`
- 验证上述步骤网络是否可达，如果可达，以上步骤配置完成。
- 如果不可达，验证 ocloud-tcenter-mc-idplogin pod 容器是否可以外网或者是否可访问企业cas server网络，网络上可达域名上不可达，则在kube-dns配置上访问的域名，如果网络不可达则联系部署交付实施配置网络与企业网络能正常连通。

6. 配置并开启之后，用户在租户端登录时，需输入主账号ID，目前企业认证登录信息是租户粒度的配置，即每个租户可配置自己的账号server，所以需先输入主账号ID，平台根据主账号ID查询对应的server信息；输入正确的主账号ID之后，平台会自动重定向到企业server端，若用户在server端是已登录状态，则直接以登录态进入控制台；若用户在server端是非登录态，则平台会打开server端登录页，用户需在server端的登录页输入账号密码在server端登录之后，再以登录态进入控制台



接入LDAP

1. 进入亿算云平台租户端控制台 ，点击【访问管理】>【企业认证登录管理界面】 页面。



2. 配置企业用户认证LDAP相关信息。

   其中，服务器地址、连接类型、基本目录、管理员账号、管理员密码、过滤条件请参考LDAP协议说明



- 用户信息字段匹配的意义说明：

  LDAP server端需将账号server端的用户信息传给平台，用户信息包括用户名、用户昵称、手机号码和邮箱。对于同样的信息，不同server返回的字段名可能不一样，接入方可在用户信息字段匹配这里对字段名做转换，

其中，json里的key表示平台读取的字段，value表示server端返回的字段名，举个例子，若server端返回的用户信息里，用户名字段命名的是user，则value里直接填value，若取的字段名是userName，则value里填写userName

- 账号同步字段意义说明：

  server端需将用户信息传给平台，平台取server端传过来的用户名之后，会检测当前租户下，是否有同名子用户，若平台存在同名子用户，则直接以该子用户身份登录到平台，若当前租户下不存在同名子用户，则会判断账号同步开关是否开启，若账号同步开关开启，则平台会在当前租户下自动创建一个同名子用户，若账号同步开关关闭，则平台会提示，平台不存在子用户，需联系管理员创建（如下图所示）

- LDAP连接测试

  配置好之后，可输入server端的账号名和密码做测试，测试成功，则显示测试成功（如图所示）



若测试失败，则会 根据失败原因显示不通失败信息





3. 配置并开启之后，用户在租户端登录时，需输入主账号ID，目前企业认证登录信息是租户粒度的配置，即每个租户可配置自己的账号server，所以需先输入主账号ID，平台根据主账号ID查询对应的server信息



4. 输入主账号ID之后，需用户再输入该用户在LDAP server端的账号密码，平台会用用户输入的账号密码去server端验证，验证成功之后，则以登录态进入控制台，验证失败则无法进入控制台


LDAP登录
登录

企业微信账号

最近更新时间: 2024-12-19 17:12:00

1. 联合账号

联合账号用来获取企业微信成员账号信息。

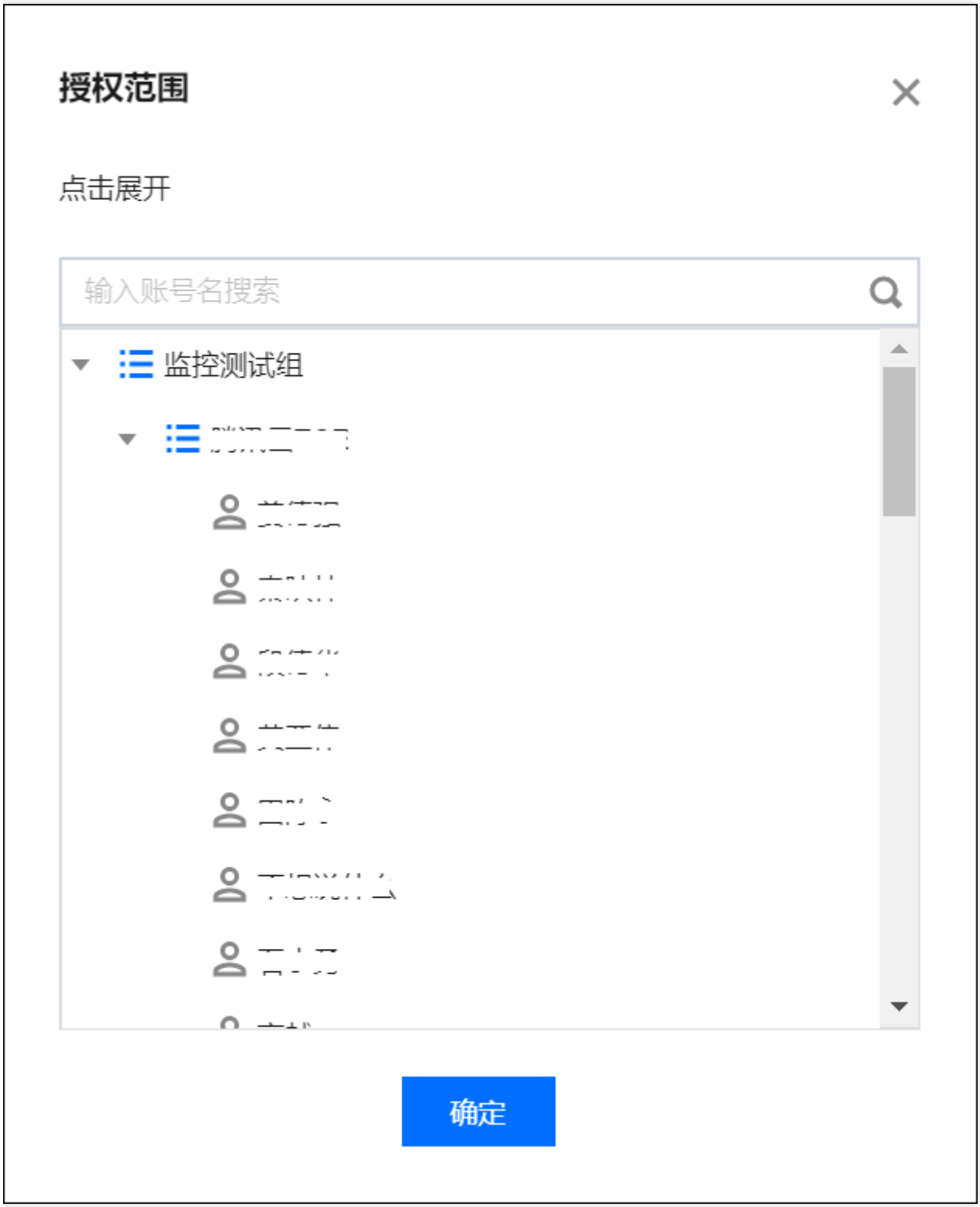
1.1 企业微信

1. 用户需要先注册企业微信，并创建企业微信的“自建应用”。
2. 获取企业微信及自建应用的相关信息：Corpid、AgentId、CorpSecret。
3. 登录云平台，进入【访问管理】>【联合账号】>【企业微信】管理页面。
4. 点击【关联企业微信账号】，将弹出“关联企业微信账号”对话框。
5. 在对话框汇总输入：AppName、Corpid、AgentId、CorpSecret



1.2 查看企业微信成员

1. 登录云平台，进入【访问管理】>【联合账号】>【企业微信】管理页面。
2. 企业微信信息列表中，点击【点击查看】，查看“自建应用”的企业微信授权成员。

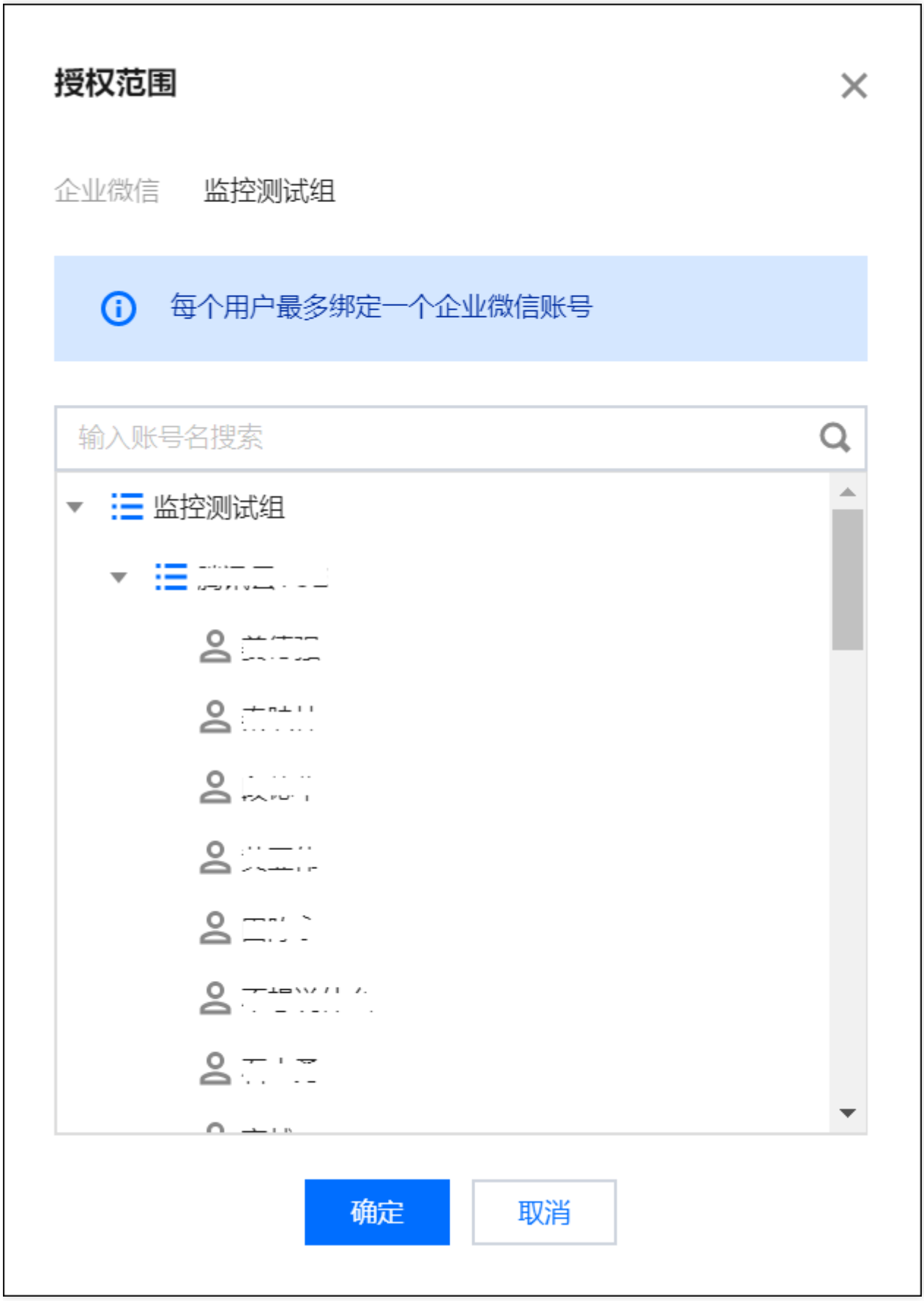


2. 用户

将企业微信成员的账号信息关联云平台用户，以便能够通过这些账号信息将消息发送给云平台用户的企业微信。

2.1 用户账号关联企业微信

1. 登录云平台，进入【访问管理】>【用户】管理页面。
2. 在用户列表的“操作”栏点击【关联企业微信】，将弹出企业微信成员对话框。
3. 在对话框汇选择要关联的企业微信成员。


授权范围
企业微信
监控测试组
每个用户最多绑定一个企业微信账号
输入账号名搜索
监控测试组
确定
取消

4. 点击【确定】完成配置。

运维手册
架构及模块说明

最近更新时间: 2024-12-19 17:12:00

1 产品介绍

访问控制（Cloud Access Management，CAM）是云平台提供的Web服务，主要用于帮助客户安全管理云平台账户下的资源的访问权限。用户可以通过 CAM 创建、管理和销毁用户(组)，并使用身份管理和策略管理控制其他用户使用云平台资源的权限。

访问管理包括四个子模块：用户管理、云api密钥，策略管理，企业认证登录管理。用户管理可以创建子账户或用户组，并将主账户/子账户加入用户组中。通过创建云api密钥，可以使用密钥通过云api无限制地访问用户的云资源。策略管理模块用于创建及编辑访问控制策略，一个策略关联到用户/用户组，从而对用户进行灵活的权限控制。企业认证登录管理提供了通过企业账户登录云的能力，只需要按照介入文档完成接入流程即可。

2 技术优势

通过访问管理单一入口对账号进行集成统一管理，轻松易用，能做到精准权限配置，最小化 管理账户 权限粒度。

2.1 根账号资源的授权访问

可以将根账号的资源授权给其他人员，包括子账号或者其他根账号，而不需要分享根账号相关的身份凭证。

2.2 精细化的权限管理

可以针对不同的资源授权给不同的人员不同的访问权限。例如可以允许某些子账号拥有某个cos存储桶的读权限，而另外一些子账号或者根账号可以拥有某个co s存储对象的写权限等。这里的资源、访问权限、用户都可以批量打包。

2.3 最终一致性

cam目前支持多个地域，通过复制策略数据实现跨地域数据同步，虽然cam策略的修改会及时提交，不过跨地域的策略同步会导致策略生效的延迟；同时cam适用缓存来提高性能（目前是一分钟缓存），更新在缓存期后生效。

3 产品架构

3.1架构

cam包括授权和鉴权两个部件。授权部件完成用户策略的管理，鉴权部件完成云api的鉴权。

授权部分通过tce控制台访问管理模块进行策略部署，cam_grant将策略写入策略cdb。用户通过控制台或者直接调用业务api，业务api西安进行鉴权，鉴权通过后才能调用具体的业务服务接口。

cam依赖的外部服务有两个:

1. 密钥服务

   完成身份认证

2. cdb存储。

   分布式存储策略，供cam_auth适用。

3.2 部署

目前在租户端和运营端，分别独立部署了一套cam系统，用于租户和运营人员的相关策略管理。目前cam主要用于tce3.0体系内部组件的权限管理相关。

4 产品详细设计

4.1 用户管理

专有云的用户帐号分为主帐号和子帐号，不同的租户对应不同的主帐号，一个主帐号下面可以带多个子帐号。一个子帐号也可以挂在多个主帐号下面，这样的用户在登录时需要选择使用哪个主帐号。在访问管理中可以添加子账号。

专有云支持添加用户组，可以把有相同权限、职责的用户放入同一个用户组。在访问管理中可以在一个用户组中添加、删除用户。

云平台主账号可通过用户管理功能对具有不同职责的分类用户进行管理。用户类型包括消息接收人、子用户等。

用户类型	登录云平台控制台	使用云平台api	策略授权	消息通知
消息接收人	不支持	不支持	不支持	支持
子用户	支持(可选)	支持(可选)	支持	不支持

4.1.1 创建子账户

1. 创建子账户(AddSubAccount)
2. 验证验证码
3. 校验当前登录用户所拥有的子账户不能超过1000个
4. 判断登录用户账号是否是开发商账号的全局管理员

5. 与主账号绑定，存储子账户属性。
6. 创建登录用户
7. 将用户添加到用户组(AddUserToGroup)
8. 判断登录用户账号是否是开发商账号的全局管理员，如果不是返回异常。
9. 将用户与用户组进行关联起来。

4.1.2 创建用户组

1. 判断登录用户账号是否是开发商账号的全局管理员，如果不是返回异常。
2. 根据uin判断用户是否存在。
3. 如果组名已存在，返回异常。
4. 创建用户组。

4.2 策略管理

策略管理包括权限、策略和授权管理。

1. 权限。描述在某些条件下允许或拒绝执行某些操作访问某些资源。
2. 策略。定义和描述一条或多条权限的语法规范。CAM支持两种类型的策略，预设策略和自定义策略。预设策略是由云平台创建和管理的一些常见的权限集合，如超级管理员、云资源管理员等，这类策略只读不可写。自定义策略是由用户创建的更精细化的描述对资源管理的权限集合。预设策略不能具体描述某个资源，粒度较粗，而自定义策略可以灵活的满足用户的差异化权限管理需求。
3. 用户或者用户组可以绑定一个或多个策略完成授权。被授权的策略既可以是预设策略也可以是自定义策略。授权方式可以通过在策略页面选择用户或者在用户页面选择策略来完成。

策略（权限）由四部分构成，分别是effect（效力）、resource_name（资源）、action（操作）、condition（授权条件）。

```
{
"effect": "allow",
"action": "*",
"resource": "*",
"condition": {
"for_any_value:string_equal": {
"qcs:tag": [
"ttttag&123"
]
}
}
}
```

4.2.1 创建策略

有三种策略创建方式：按策略生成器创建，按策略语法创建，按标签创建。

4.3 云api密钥管理

每个账户最多创建两个密钥，每个密钥包括SecretId和SecretKey，由系统自动生成。可以在管理中禁用密钥，只有禁用的密钥可以进行删除操作。

4.3.1 创建密钥

由云api负责创建。

后端标识：tcloud-tcenter-cam

请求参数：uin，

应答：secretProjectId, secretId, status。

5 功能模块组件对应表

功能	模块	组件	功能组件说明	备注
权限	权限管理	tcloud-tcenter-cam	负责授权读写、鉴权、密钥等	

运维工具介绍

最近更新时间: 2024-12-19 17:12:00

无特殊工具，只需要通过ssh登陆机器，通过kg tag / kg命令找到对应服务的容器，进入之后执行相关操作即可。

日常巡检

最近更新时间: 2024-12-19 17:12:00

1 服务可用性检查

通过对服务的域名+端口进行curl，验证cam各服务是否正常。例如:kg tcloud-tcenter-platform-waccount，找到容器IP，比如: 192.168.241.176 curl -v -d '' http://192.168.241.176:50030 header 状态码返回 200，则表明访问服务正常。

2 服务健康性检测

登陆租户端，进入访问管理控制台能够正常拉取出用户列表和用户组列表，以及对策略可以成功进行绑定。

1. 进入访问管理控制台，可以成功创建子账户及用户组
2. 可以正常把子账户关联到一个用户组
3. 可以正常创建一个策略
4. 可以正常将策略关联到用户
5. 对用户访问管理的策略可以正常生效

版权所有：亿算云平台

故障处理

最近更新时间: 2024-12-19 17:12:00

导入cam数据失败

故障现象

租户端导入cam数据后，服务不可见。

故障影响

无法导入预设策略。

故障处理

目前是通过白名单字段控制，如whiteKey，如果开放的话，将此字段置为空即可：

```
mysql> select * from cService where serviceType in ('dcdb','mariadb')\G;
*************************** 1. row ***************************
serviceType: dcdb
serviceName: 分布式数据库 DCDB
isDisZone: 1
isDisProject: 1
isSeen: 0
queryAddr: [{"region":"def","url":" "}]
weight: 18
writter: byronzhong
addTime: 2018-04-18 11:00:48
updateTime: 2018-11-22 18:24:36
queryInterface:
synInterface:
isAllowDefProj: 1
serviceEnName: DCDB
colConf: ""
defAddr:
whiteKey: dcdb_cam
defaultStrategyList:
arnDocument:
*************************** 2. row ***************************
serviceType: mariadb
serviceName: 云数据库 MariaDB（TDSQL）
isDisZone: 1
isDisProject: 1
isSeen: 0
queryAddr: [{"region":"def","url":" "}]
```

```
weight: 17
writter: byronzhong
addTime: 2018-04-18 10:56:45
updateTime: 2018-11-22 14:30:19
queryInterface:
synInterface:
isAllowDefProj: 1
serviceEnName: CDB for MariaDB（TDSQL）
colConf: ""
defAddr:
whiteKey:
defaultStrategyList:
arnDocument:
2 rows in set (0.00 sec)
```

查询持久密钥异常

故障现象

前端页面提示qcloud.Qsecret.queryKey错误。

故障影响

无法获取持久密钥，影响服务鉴权。

故障处理

一般是 cam 临时会话服务(sts)访问出错或者云安全模块持久密钥服务访问出错。

1. 检查cam-sts 50020端口 是否可以访问，如果无法访问，检查域名解析是否故障，以及tcloud-tcenter-cam容器是否启动。
2. 如果步骤1没有问题，检查cam-apisig的ip:port是否可以访问，联系云安全模块运维人员进行处理。

控制台身份校验失败

故障现象

前端页面提示GET_SESSIONTOKEN_FAILED check sig error。

故障影响

控制台不可用。

故障处理

出现该结果原因是cam鉴权服务校验控制台身份失败。

1. 查看STS模块日志（路径：/data/log/sts/sts/detail/）。
2. 检查cam-apisig的ip:port是否可以访问，如果访问异常，联系云安全模块运维人员进行处理，否则跳转到步骤3。
3. 检查控制台配置的conSecretId和conSecretKey是否正确，联系运维人员分配新的conSecretId和conSecretKey。

临时密钥获取异常

故障现象

前端页面提示GET_SESSIONTOKEN_FAILED system erro。

故障影响

控制台不可用。

故障处理

出现该结果原因是sts服务访问db失败或者访问cam临时秘钥模块失败。

1. 查看STS模块日志（路径：/data/log/sts/sts/detail/），如果日志显示访问访问db失败，查看db配置是否正确；
2. 如果日志显示tcp error （端口为50023），查看cam秘钥种子服务ip:port是否配置正确（配置文件路径/data/release/swoole_sts/application/config/idc/hosts_config.php 配置为REGIONINDEX），如果配置正确，查看tcloud-tcenter-cam的pod是否正常启动、网络是否正常。

云api鉴权失败

故障现象

云api返回鉴权失败，错误码为4100。

故障影响

下游服务接口调用失败

故障处理

出现结果原因是cam鉴权服务校验身份失败。

1. 检查云api模块配置的鉴权访问是否正确，正确配置为auth.cam.logical.server.console.tencentyun.com:9502。

2. 检查cam鉴权模块auth.cam.logical.server.console.tencentyun.com:9502是否可以访问。
3. 检查云安全模块ip:port是否可以访问。
4. 如果以上步骤没有问题，请检查调用方的conSecretId和conSecretKey是否正确。

策略校验异常

故障现象

绑定了相关策略，仍返回鉴权失败。

故障影响

资源不可用，或服务接口请求失败。

故障处理

1.检查该账户绑定的策略是否包含该接口 2.如果已绑定相关策略，鉴权不符合预期参考2.6 3.角色鉴权问题参考“角色鉴权异常”。

错误提示为you are not authorized to perform operation。

1. 鉴权服务存在一分钟的缓存，请一分钟后再尝试。
2. 如果超过一分钟仍未生效，检查tcloud-tcenter-cam的pod 中 crontab 状态是否正常 service crond status。未执行尝试重启pod；

角色鉴权异常

故障处理

1. 提示角色不存在，原因是因为未创建角色，云平台目前在业务侧前端创建。
2. 用角色临时秘钥访问接口提示无权限，检查业务侧代码是否有给角色绑定策略。
3. 角色临时秘钥访问资源提示无权限，需要检查创建角色时给到的资源是否正确。

手机收不到验证信息

现象描述

在进行绑定或者修改手机号码、重置密码等操作时，手机收不到验证信息。

可能原因

导致手机收不到验证信息的主要原因包括：

- 手机号码、区号填写错误。
- 手机系统根据关键词，自动隐藏了内容。
- 手机号码自身原因导致的接收异常，如欠费、网络故障等。

处理步骤

1. 请确认手机号码是否填写正确。

- 是，请执行下一步。
- 否，请 修改手机号码。

2. 请核实手机是否已停机。

- 是，请进行缴费或者更换手机号码。
- 否，请执行下一步。

3. 请确认验证信息是否被视作垃圾短信而被拦截。

- 是，请解除应用软件的短信拦截。
- 否，请执行下一步。

4. 网络通讯异常可能会造成短信丢失，请确认网络通讯是否存在异常。

邮箱收不到验证信息

现象描述

在进行绑定或者修改邮箱、重置密码等操作时，邮箱收不到验证信息。

可能原因

导致邮箱收不到验证信息的主要原因包括：

- 邮箱地址填写错误。
- 邮箱系统根据关键词，自动隐藏了内容。
- 邮箱系统存在特殊限制，导致接收失败。例如，企业的自建邮箱禁止接收第三方邮件。

处理步骤

1. 请确认邮箱地址是否填写正确。

- 是，请执行下一步。
- 否，请 修改邮箱地址。

2. 请确认验证信息是否被视作垃圾邮件，存放在垃圾箱中。

- 是，请将邮箱设置为白名单。
- 否，请执行下一步。

3. 网络通讯异常可能会造成邮件丢失，请确认网络通讯是否存在异常。

- 是，请重新获取或稍后再试。
- 否，请执行下一步。

4. 请确认邮箱地址是否为企业自建邮箱，且设置了禁止接收第三方邮件。

应急预案

最近更新时间: 2024-12-19 17:12:00

DB故障处理方案

恢复步骤

1. 单地域db故障时，可自动容灾(可能会出现个别请求超时)，如果未恢复，先快速处理，将流量切到异地，在处理异常的db。
2. 单地域db同步异常，修改db配置。
3. 需要修改配置时，找到对应集群的配置，修改后下发，修改配置重启为reload模式，无需剔除机器。

最佳实践

最近更新时间: 2024-12-19 17:12:00

未有特殊实践案例，参考巡检、故障处理等。

节点重启

最近更新时间: 2024-12-19 17:12:00

以waccount服务为例。

1. 系统重载(推荐)

```
cd /data/release/waccount/application
sh service.sh -t reload -n SWOOLE_WTAG
```

执行成功后会显示reload succ

2. 系统重启

```
cd /data/release/waccount/application
sh service.sh -t restart -n SWOOLE_WTAG
```

执行成功后会显示restart succ

节点重启后，执行 `ps aux | grep SWOOLE_WTAG` ，观察一下启动时间。

扩容指导

最近更新时间: 2024-12-19 17:12:00

1 在已有集群扩容cam_auth

1. 新机器安装swoole。
2. 创建允许user_00访问的目录/data/release/cam_swoole，将软件包同步到机器的上述目录下，同步完成后把cam_swoole下所有代码都设置为全读写状态
3. 把脚本变成可执行状态。具体命令 sudo su; cd /data/release/cam_swoole/sh; chmod 777 *
4. 鉴权策略实效性旁路工具部署(在启动鉴权服务之前部署)
5. 拷贝代码到/data/release/cam_strategy
6. 启动服务
7. 添加cmq主题订阅

2 节点扩容

当系统复杂比较高的时候，需要增加工作节点的数量。系统基于kubernetes进行容器编排及管理，扩容步骤如下：

1. 准备新机器，安装k8s环境。

2. 将新节点加入集群，命令如下：

```
kubeadm join --token [TOKEN] {master_ip}:6443 --discovery-token-ca-cert-hash sha256:[SHA256]
```

TOKEN可以通过命令 `kubeadm token list` 查看，每个token24小时有效期，

SHA256加密字符串通过命令 `openssl x509 -pubkey -in /etc/kubernetes/pki/ca.crt | openssl rsa -pubin -outform der 2>/dev/null | openssl dgst -sha256 -hex | sed 's/^.* //'` 获取。

3. 使用命令 `kubectl get nodes` 查看集群内所有节点。

3 swoole worker

当机器负载不搞，系统性能不足时，可以通过增加工作进程的数量来提高系统处理能力。

1. 登陆机器
2. kg tag
3. ke {node id}
4. cd /data/release/waccount/application
5. vim product_env.php
6. 找到WORK_NUM一行，修改对应的数字为希望扩容到的数字
7. 重启节点

备份恢复

最近更新时间: 2024-12-19 17:12:00

使用支撑MySQL作为持久化存储，依赖支撑MySQL提供的备份及恢复能力

参考信息

最近更新时间: 2024-12-19 17:12:00

1 配置文件参考

1.1 通用配置文件

1. idc/database_config.php

功能：数据库配置

样例：

```
<?php
class DatabaseConfig {

public static function getDbInfo(){
$database = array( //dict结构: db_name => 配置详情
'default' => array(
'ip' => '127.0.0.1',
'port' => 3306,
'user' => 'root',
'password' => '123456',
'charset' => 'utf8',
'mode' => 'async'
),
'qcloudTag' => array(
'ip' => '10.182.21.52',
'port' => 3300,
'user' => 'ccdb',
'password' => 'UEDh5ZVx93IOGYCs',
'charset' => 'utf8',
'mode' => 'async'
),
'qcloudTagCheck' => array(
'ip' => '10.182.21.52',
'port' => 3300,
'user' => 'ccdb',
'password' => 'UEDh5ZVx93IOGYCs',
'charset' => 'utf8',
'mode' => 'async'
),
'cAuth' => array(
'ip' => '10.182.21.52',
```

```
'port' => 3300,
'user' => 'ccdb',
'password' => 'UEDh5ZVx93IOGYCs',
'charset' => 'latin1',
'mode' => 'async'
),
);
return $database;
}

/*
* 实例名
* 库名
* 表明
*
*/
const DEFAULT_HANDLER = 'default';
const TAG_HANDLER = 'qcloudTag';
const TAG_CHECK_HANDLER = 'qcloudTagCheck';
const CAUTH_HANDLER = 'cAuth';

/*
* db 名
*
*/
const DEFAULT_DB = 'test';
const TAG_DB = 'qcloudTag';
const CAUTH_DB = 'cAuth_test';

}
```

数据库配置在物料库由工作人员统一配置，客户无需更改内容，如有变更，联系运维人员操作。

2. idc/hosts_config.php

功能：下游服务配置

样例:

```
const CMSI_URL = "http://sz.cmsi.isd.com/interface.php";// 消息服务url，用于发送短息和邮件
const ACCOUNT_URL = "http://account.tencentyun.com:50001"; // 账户服务url
static $elk_url_module = array(
self::ACCOUNT_URL => 'QC_ACCOUNT',
); //需要发送elk日志的下游服务
static $elk_all_http_report = true; //是否开启全量elk报告
```

elk_all_http_report开关打开后，会把全量的http调用日志打到elk。

1.2 授权服务(grant/grant_write)

1. module_config.php

功能：接口模块请求配置，

```
'module_frequency_time'=> 1, //模块请求统计固定间隔时间，单位s
'module_frequency_max_num'=> 1000, //模块固定时间间隔最大请求量
'module_interface_frequency_time'=> 1, //接口请求统计固定间隔时间，单位s
'module_interface_frequency_max_num'=> 400, //接口固定时间间隔最大请求量
'module_interface_frequency_field_time'=> 1, //接口请求统计固定间隔时间，单位s
'module_interface_frequency_field_max_num'=> 100, //接口固定时间间隔最大请求量
```

接口统计有一定的性能代价，高负载情况下可以适当调整阈值。

请求量的配置用于系统频控。

2. white_list.php

功能：白名单配置

```
const STRATEGY_TOTALITY_NAME = "strategy_totality";
const STRATEGY_TOTALITY_DEFAULT_MAX_NUM = 10000;

const RELATED_TOTALITY_NAME = "related_totality";
const RELATED_TOTALITY_DEFAULT_MAX_NUM = 600;

const STRATEGYINFO_LENGTH_NAME = "strategyinfo_length";
const STRATEGYINFO_LENGTH_MAX_NUM = 10000;

const COS_POLICY_LENGTH_NAME = "cos_policy_length";
const COS_POLICY_LENGTH_MAX_NUM = 30000;
```

白名单策略的一些配置，请在开发人员指导下进行变更。

1.3 账户服务(account/waccount)

1. account.php

功能：账户服务系统内部用到的配置，不可更改。

2. auth_config.php

功能：实名认证相关配置。

```
const addrTag = '_ad!@#ad_';

const AUTH_INTERVAL_TIME = 30; //两次认证间隔时间必须超过30天
const AUTH_MAX_TIMES = 3; //同一个认证主体最多认证三次

#认证统一标志
const USER_PASS_AUTHENTICATE = 1;
const USER_NOT_AUTHENTICATE = 0;

#银行卡的状态
const BANK_STATUS_SUBMIT = 0;//提交
const BANK_STATUS_SENDED = 1;//发送给teg
const BANK_STATUS_PASS = 2;//认证通过
const BANK_STATUS_FAIL = 3;//认证失败
const BANK_STATUS_SUCCESS = 4;//打款成功
const BANK_STATUS_CLEAR = 5;//清空信息
const BANK_STATUS_WAITING = 33;//待确认

#实名表的状态
const CHECK_STATE_NOT_SUBMIT = 0;//未提交
const CHECK_STATE_AUDITING = 1;//审核中
const CHECK_STATE_NOT_PASS = 2;//未通过
const CHECK_STATE_PASS = 3;//通过
const CHECK_STATE_WAITING = 33;//待确认

#实名认证状态
const USER_AUTHENTICATE_EVEN_NOT = 0;//未认证
const USER_AUTHENTICATE_AUDITING = 1;//审核中/认证中
const USER_AUTHENTICATE_WAITING = 33;//待确认
const USER_AUTHENTICATE_NOT_PASS = 2;//不通过
const USER_AUTHENTICATE_PASS = 3;//通过/已认证

#实体类型
const TYPE_PERSONAL = 0;//个人
const TYPE_ENTERPRISE = 1;//企业

const AREA_MAINLAND = 0;//大陆
const AREA_HK_MACAO = 1;//港澳
const AREA_TAIWAN = 2;//台湾
const AREA_OVERSEAS = 3;//外藉

#实名认证方式
const AUTHTYPE_UNKNOWN = 0;//未知
const AUTHTYPE_INFORMATION_SUBMIT = 1;//提交资料审核认证
const AUTHTYPE_TENPAY = 2;//个人财付通，老的已下线
const AUTHTYPE_ENTERPRISE_BANK = 3;//企业银行卡
const AUTHTYPE_PERSONAL_WECHAT = 4;//微信
```

```
const AUTHTYPE_PERSONAL_QQ_MOBILE = 5;//手Q
const AUTHTYPE_ENTERPRISE_WECHAT = 6;//企业微信
const AUTHTYPE_OFFLINE = 7;//线下认证
const AUTHTYPE_INTERNATIONAL_CREDITCARD = 8;//国际信用卡
```

AUTH_INTERVAL_TIME 和 AUTH_MAX_TIMES两个配置可修改。

3. token_config.php

功能： 账户登陆所拥有token相关配置属性。

```
const LOGIN_TOKEN_VALID_TIME = 60; // 登陆token有效时常，单位秒
const BIND_TOKEN_VALID_TIME = 600; // 绑定的qq/wx登陆时token的有效时长，单位秒
const COLL_PHONE_VERIFY_TOKEN_VALID_TIME = -1;// 电话绑定登陆token的有效时长，单位秒
const MINA_CODE_TOKEN_VALID_TIME = 3600; // s
const SUB_ACCOUNT_LOGIN_TOKEN_VALID_TIME = 600; // 子账户登陆有效时长
const SUB_ACCOUNT_SECRET_TOKEN_VALID_TIME = -1; //子账户密钥登陆有效时长
```

2 日志文件参考

日志目录： /data/log/{service_name}

目录下有5个子目录,下面分别进行介绍。

1. acc。http调用日志，文件粒度：日。

```
2020-12-14 11:09:13|BaseHttpClientService|1170|100003|[SWOOLE_WTAG] sys_err:http error //http调用失败。

2020-12-14 11:10:58|BaseHttpClientService|14883|0|ok //http调用成功
```

2. db。数据库执行系统日志，文件粒度: 小时。

```
[2020-12-14 15:46:29][getDb][229][[get handler][event id :0][try to fetch platform-account.qcloudTag.utf8 db handler][pid:403115][cur conn:1][idil num:1]]
[2020-12-14 15:46:29][getDb][241][[result handler][event id :0][platform-account.qcloudTag.utf8:conn suc]]
```

3. req。服务请求日志，文件粒度：小时。

```
[2020-12-14 17:53:50][INFO][001001606462335130871 9][DispatchUtil][dispatch][19][REQUEST : {"version":"v1.0.0","componentName":"CDB","eventId":1607939630,"timestamp":1607939630396,"interface":{"interfaceName":"qcloud.tag.addResourceTag","para":{"uin":100004604168,"createUin":100004604168,"tagKey":"tbase_key1","tagValue":"tbase_value1","resource":"qcs::ctsdb:chongqing:uin/100004604168:instance/ctsdb-81u2cnm3d"}}} [{"remote_port":57640,"remote_addr":"192.168.241.122","real_ip":""}]] // 请求日志，包含请求参数，服务接口名，上游地址，上游服务等信息
[2020-12-14 17:53:53][INFO][001001606462335130871 9][DispatchUtil][format_output][125][RESPONSE : {"version":"v1.0.0","timestamp":1607939630396,"eventId":1607939630,"componentName":"SWOOLE_WTAG","returnValue":0,"returnCode":0,"returnMessage":"ok","interface":"qcloud.tag.addResourceTag","data":[]}] //应答日志。
```

4. sys。系统框架日志。文件粒度：日。

```
[2020-12-14 01:20:22][ERROR][001001606462335130871 9][main][{closure}][42][SWOOLE_WTAG_worker start [pid:661703]]

// swoole框架启动日志，worker进程启动了
```

5. detail。业务日志。文件粒度: 小时。

业务代码里的日志都在这里，当需要观察业务调用流程时，可以查看本日志。当出现异常时，也可以在这里查看堆栈日志。

```
[2020-12-14 18:01:58][ERROR][001001606462335130871 9][HttpAccountService][sendRequest][42][HttpAccountService_sendRequest_response======>>>{"code":0,"res_info":"ok","data":"{\"version\":1,\"timestamp\":1607940118,\"eventId\":\"\",\"componentName\":\"SWOOLE_WHITELIST\",\"returnValue\":0,\"returnCode\":0,\"returnMessage\":\"ok\",\"
interface\":\"qcloud.Qconfig.qconfigBatchGetWhiteList\",\"data\":[]}","msg":"ok"}]
[2020-12-14 18:01:58][INFO][001001606462335130871 9][BaseDbService][_execute][68][[sql begin] [event_id:0] [sql:SELECT count(*) as cnt FROM qcloudTag.tagResourceRelate WHERE uin = '100004606348' AND region = 'chongqing' AND serviceType = 'cvm' AND resourcePrefix = 'instance' AND resourceId = 'ins-bg4yrcyd']]
[2020-12-14 18:01:58][INFO][001001606462335130871 9][BaseDbService][_execute][149][[sql result] [event_id:0] [sql:SELECT count(*) as cnt FROM qcloudTag.tagResourceRelate WHERE uin = '100004606348' AND region = 'chongqing' AND serviceType = 'cvm' AND resourcePrefix = 'instance' AND resourceId = 'ins-bg4yrcyd'] [result:{"code
":
```

3 性能指标

1. 用户列表查询 pct99: 300ms。
2. 新建 pct99: 1s。
3. 用户组列表 pct99: 300ms。
4. 新建用户组 pct99: 1s。
5. 策略列表 pct99:200ms。
6. 新建自定义策略 pct99: 1.5s。
7. 策略绑定用户 pct99: 800ms。
8. cpu使用率 5%。
9. 内存占用率 10%。

4 技术指标

1. 用户创建成功率 99.9%
2. 用户组查询成功率 99.9%
3. 策略创建成功率99.9%
4. 策略绑定成功率99%