访问管理

产品文档

版权所有：建行云

文档目录

- 产品简介
  - 访问控制概述
  - 产品功能
  - 应用场景
  - 使用限制
  - 支持CAM的产品
- 操作指南
  - 概述
  - 用户
    - 用户类型
    - 主账号
    - 子用户
    - 用户信息
    - 用户设置
  - 访问密钥
  - 用户组
    - 新建用户组
    - 用户管理
    - 用户组权限设置
  - 策略
    - 相关定义
    - 授权指南
    - 语法逻辑
- 排除故障
  - 如何根据故障反馈创建策略
- 企业认证登录管理
  - 接入准备
  - 接入步骤
- 相关案例
  - CVM相关案例

版权所有：建行云

产品简介
访问控制概述

最近更新时间: 2023-09-07 14:29:56

访问控制是云平台提供的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。用户可以通过访问控制创建、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。

版权所有：建行云

产品功能

最近更新时间: 2023-09-07 14:29:56

访问控制提供以下功能支持：

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，包括子账号或者是其他根账号，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。

版权所有：建行云

应用场景

最近更新时间: 2023-09-07 14:29:56

租户子账号权限管理

子账号最小化访问权限。 场景：某个主账号下拥有很多云资源，包括CVM 、VPC实例、CDN实例、COS存储桶和对象等。该账号下资源由员工共享，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。

版权所有：建行云

使用限制

最近更新时间: 2023-09-07 14:51:29

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	10
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	1500
一个策略语法最大字符数	4096

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。

版权所有：建行云

支持CAM的产品

最近更新时间: 2023-09-07 14:51:29

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控制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访问控制的服务。 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。

o 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。

o 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。

o 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	✓	✓	–	–
容器服务	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	✓	✓	–	–
文件存储	资源级	✓	–	–	–
云硬盘	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	✓	–	–	–

版权所有：建行云

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
私有网络	资源级	✓	–	–	–

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
MYSQL增强版	资源级	✓	–	–	–
Redis增强版	资源级	✓	–	–	–
云数据库Oracle版	操作级	✓	–	–	–
云数据库Oracle 专用版	操作级	✓	–	–	–

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	✓	–	–	–
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	✓	–	–	–

版权所有：建行云

操作指南

概述

最近更新时间: 2023-09-07 14:58:19

详细描述了CAM的核心能力以及使用方法。包括身份管理、策略管理和策略语法这几部分，并对CAM的一些使用限制进行了说明。

版权所有：建行云

用户
用户类型

最近更新时间: 2023-09-08 09:08:44

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户、及消息接收人。

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	✔	✔	-
策略授权	默认已拥有全部策略	✔	-
消息通知	✔	✔	✔

主账号

最近更新时间: 2023-09-07 15:12:18

账号主相关

操作场景

本文档介绍主账号权限设置与消息接收，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（CAM）– 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。

版权所有：建行云

子用户

最近更新时间: 2023-09-07 15:12:17

新建子用户

创建子用户

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。需要特别注意建行云子用户新建完成后默认开通登录短信二次认证，请您务必注意预留手机号码的准确性。

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】，进入用户管理页面。

2. 在用户管理页面，单击【新建用户】，进入新建用户页面。

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）、备注、手机、邮箱信息。

说明

o 单击【添加用户】可一次最多创建10个用户。

o 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。

o 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。

o 云控制台访问：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，建行云已强制开启短信二次认证登录保护。

5. 单击【下一步：设定权限】，进入设置用户权限页面。

6. 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。

o 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。

o 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。

o 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。

7. 单击【下一步：完成】。

8. 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。

9. 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。

o 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

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，进入 用户列表 管理页面。
2. 在用户列表管理页面，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，进入用户组管理页面。
2. 在用户列表管理页面，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，进入 用户列表 管理页面。
2. 在用户列表管理页面，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，进入用户组管理页面。
2. 在用户列表管理页面，点子用户名，进入用户详情页。
3. 单击【已加入的用户组】可以查看该用户加入的用户组。
4. 在用户组操作栏，找到需要移出的用户组
5. 单击右侧操作列的【移出该组】--【确认移出】，完成通过从组中解除子用户关联策略的操作。

子用户安全凭证

子用户登录

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。

版权所有：建行云

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：10000460####）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

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】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。

o 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。

o 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

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】，进入用户管理页面。

2. 在用户列表管理页面，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】，进入用户列表管理页面。

2. 在用户列表管理页面，选择需要设置安全保护的子用户。

版权所有：建行云

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。

子用户订阅消息

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

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，进入 用户列表 管理页面。

操作步骤

删除单个子用户

1. 在用户列表管理页面，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。

版权所有：建行云

用户信息

最近更新时间: 2023-09-07 15:21:39

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，进用户管理页面，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，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。

o 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。

o 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。

o 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。

版权所有：建行云

用户设置

最近更新时间: 2023-09-07 15:21:39

密码规则

操作场景

本文档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【账号中心】> 【安全设置】，进入安全设置页面。
2. 点击【密码期限设置】模块的编辑按钮，可以修改密码的有效期限，其中0天表示不限制，最长可设置 365 天。
3. 单击【确定】按钮完成密码期限设置。从上一次修改密码开始计算，到达有效期需要重置密码。

版权所有：建行云

访问密钥

最近更新时间: 2023-09-07 15:21:39

查看当前用户访问密钥

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 API 密钥管理页面。

操作步骤

主账号或具有 QcloudCollApiKeyReadOnlyAccess 策略 权限的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 QcloudCollApiKeyManageAccess 策略 权限。

版权所有：建行云

用户组

新建用户组

最近更新时间: 2023-09-07 15:28:26

新建用户组

1. 登录访问管理控制台，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。

版权所有：建行云

用户管理

最近更新时间: 2023-09-07 15:28:26

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，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。

版权所有：建行云

用户组权限设置

最近更新时间: 2023-09-07 15:28:26

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，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：建行云

策略

相关定义

最近更新时间: 2023-09-07 15:48:24

权限

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

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。

版权所有：建行云

授权指南

最近更新时间: 2023-09-08 09:42:19

创建自定义策略

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。

o 服务（必选）：选择需要添加的产品。

o 操作（必选）：选择您要授权的操作。

o 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」。

o 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。

o 赋予用户/用户组：勾选需要授权的用户/用户组。（可选其一）

o 在标签键：选择需要授权的标签键。（必填项）

o 且具有标签值：选择需要授权的标签值。（必填项）

o 的资源：默认为管理权限。

3. 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。

4. 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

操作场景

本文档介绍如何通过策略关联用户/用户组和如何通过用户/用户组关联策略。关联成功后，用户/用户组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：

通过预设策略关联用户

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，单击【策略类型】>【预设策略】，筛选预设策略，如下图所示：

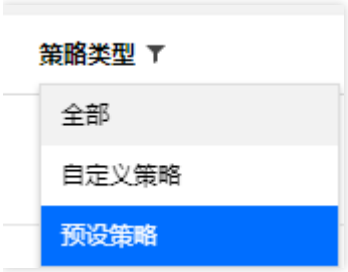
3. 找到需要授权的预设策略，单击右侧操作列的【关联用户/组】，如下图所示：

4. 在弹出的关联用户/用户组窗口，单击【类型】>【用户】，如下图所示：

5. 勾选要关联的用户，单击【确定】，完成通过预设策略关联用户操作。

通过预设策略关联用户组

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，单击左上角【策略类型】>【预设策略】，筛选预设策略，如下图所示：



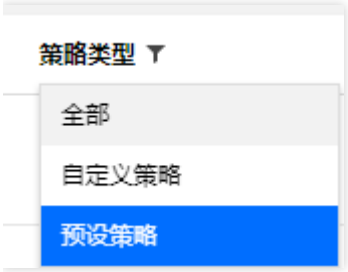
3. 找到需要授权的预设策略，单击右侧操作列的【关联用户/组】，如下图所示：

4. 在弹出的关联用户/用户组窗口，单击【切换用户组】>【用户组】，如下图所示：

5. 勾选要关联的用户组，单击【确定】，完成通过预设策略关联用户组操作。

自定义策略关联用户

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，单击左上角【策略类型】>【自定义策略】，筛选自定义策略，如下图所示：



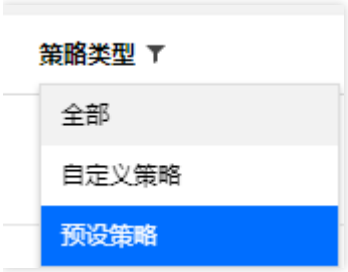
3. 找到需要授权的自定义策略，单击右侧操作列的【关联用户/组】，如下图所示：

4. 在弹出的关联用户/用户组窗口，单击【切换用户组】>【用户】，如下图所示：

5. 勾选要关联的用户，单击【确定】，完成通过自定义策略关联用户操作。

通过自定义策略关联用户组

1. 在访问管理控制台，单击左侧【策略】，进入 策略管理页面。
2. 在策略管理页面，单击左上角【策略类型】>【自定义策略】，筛选自定义策略，如下图所示：



3. 找到需要授权的自定义策略，单击右侧操作列的【关联用户/组】，如下图所示：

4. 在弹出的关联用户/用户组窗口，单击【切换用户组】>【用户组】，如下图所示：

5. 勾选要关联的用户组，单击【确定】，完成通过自定义策略关联用户组操作。

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 用户详情 页面。
2. 在【已关联的策略】下面点击【关联策略】。
3. 在策略列表中选择策略。
4. 勾选需要授权的策略，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 用户组管理页面。
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. 在用户组详情页，单击【已关联的策略】，进入权限设置页面。
4. 在权限设置页面，单击【关联策略】。
5. 在弹出的关联策略窗口中，单击【策略类型】>【预设策略】，筛选预设策略/自定义策略，如下图所示：

6. 勾选需要授权的预设策略，单击【确定】，完成通过用户组关联预设策略操作。

限制IP访问

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。

o 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。

o 服务：必填项，选择需要添加的产品。

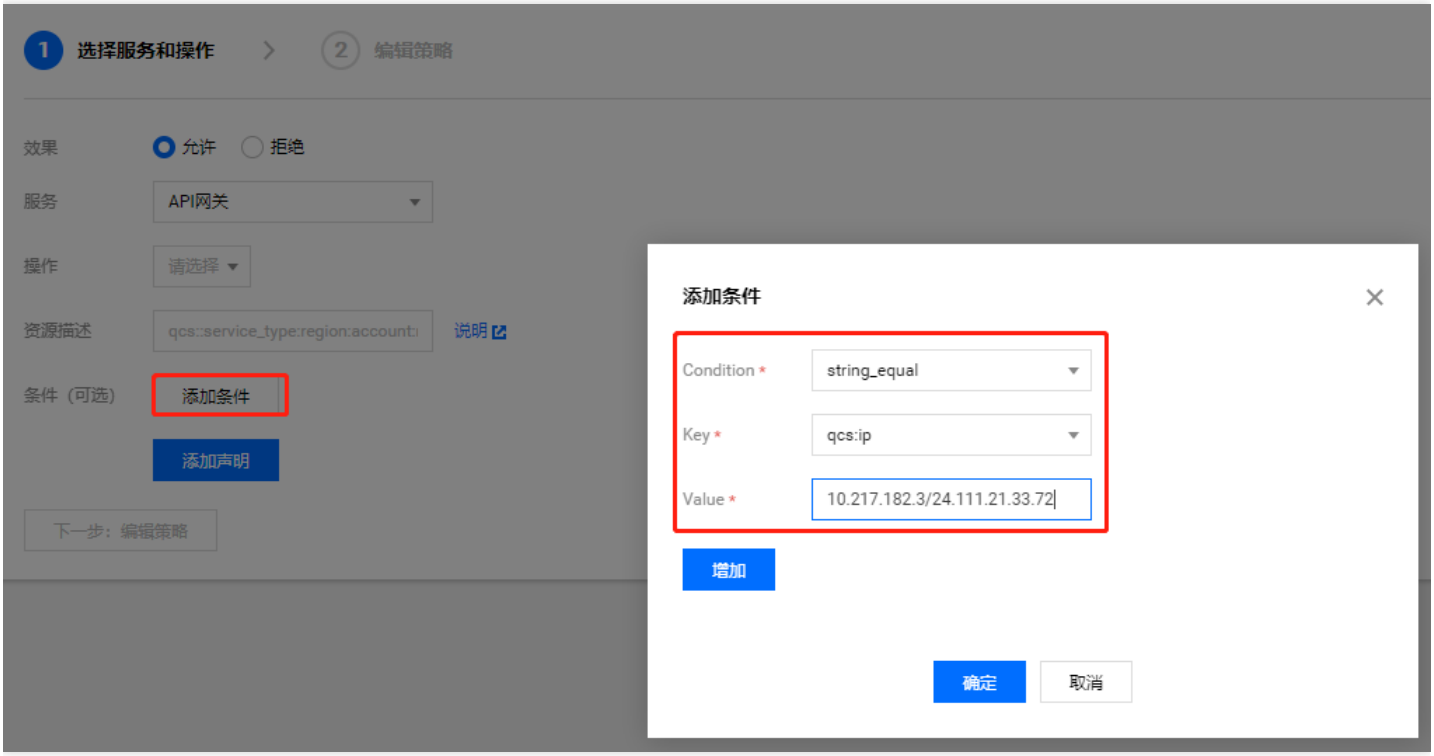
o 操作：必填项，根据您的需求勾选产品权限。

o 资源：必填项，您可以参考 资源描述方式填写。

o 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"
                    ]
                }
            }
        }
    ]
}
```

wuxiaoyu2.zh

语法逻辑

最近更新时间: 2023-09-08 11:25:43

元素参考

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

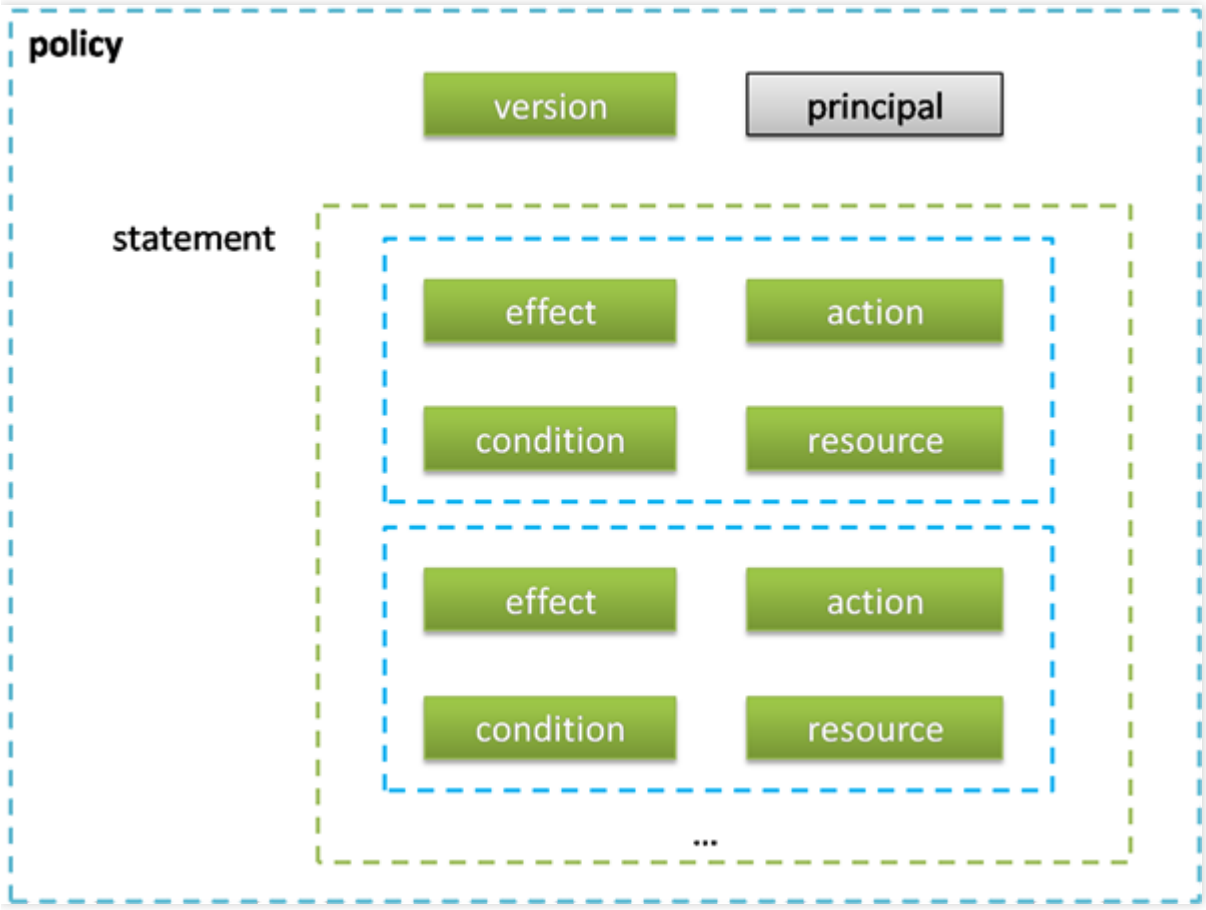
该样例描述为：允许属于开发商 ID 1238423下的子账号 ID 3232523以及组 ID 18825， 对北京地域的cos存储桶 bucketA和广州地域的 cos 存储桶 bucketB 下的对象 object2，在访问 IP 为10.121.2.*网段时，拥有所有 cos 读

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:wh:uid/1238423:prefix//1238423/bucketA/*",
                "qcs::cos:wh: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

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>, ...]

= { , > , ... } 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”:

• 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” : ”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>)<principal_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

project目前不区分，不填具体字段。

示例如下所示：

// COS 产品的 object 资源，武汉地域，资源拥有者的 uid 是100004601234，资源名是 bucket1/object2 ，资源前缀是 prefix qcs::cos:wh:uid/100004601234:prefix//100004601234/bucket1/object2

// CVM 产品的云服务器，武汉地域，资源拥有者的uin是100004601234，资源名是 ins-abcdefg,资源前缀是 instance qcs::cvm:wh:uin/100004601234: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":["wh","bj"]},
        "ip_equal":{"qcs:ip":"10.131.12.12/24"}
}
```

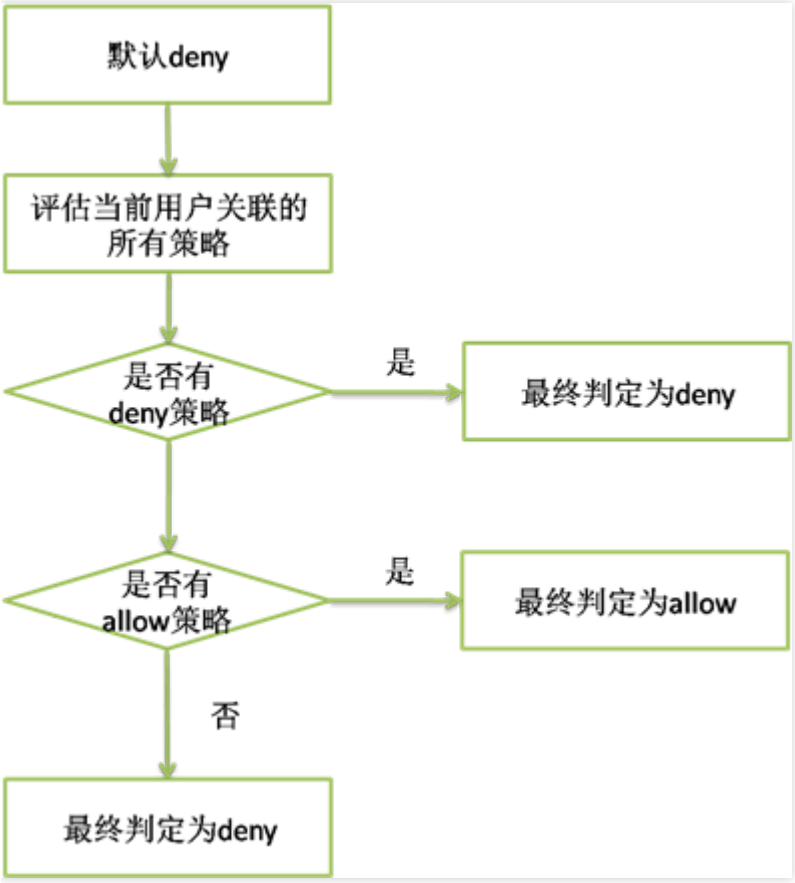
condition_key_string 条件键，表示将对其值采用条件操作符进行操作，以便确定条件是否满足。CAM 定义了一组在所有产品中都可以使用的条件键，包括 qcs:current_time、qcs:ip 、qcs:uin 和 qcs:owner_uin 等。具体信息请参阅 生效条件。

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 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。

i. 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。

ii. 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。

iii. 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"}}
	}

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

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

版权所有：建行云

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
wh	武汉
bj	北京

• 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。

o uin 方式，即根账号的 QQ 号，表示为uin/${uin}，如 uin/12345678；

o uid 方式，即根账号的 APPID，表示为uid/${appid}，如 uid/10001234。

*o 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。

a. 表示某个资源子类下的资源 ID 。如 VPC 产品的 instance/ins-abcdefg。

/

b. 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 。

/

b. 表示某个资源子类下的所有资源。如 instance/。

/

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

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

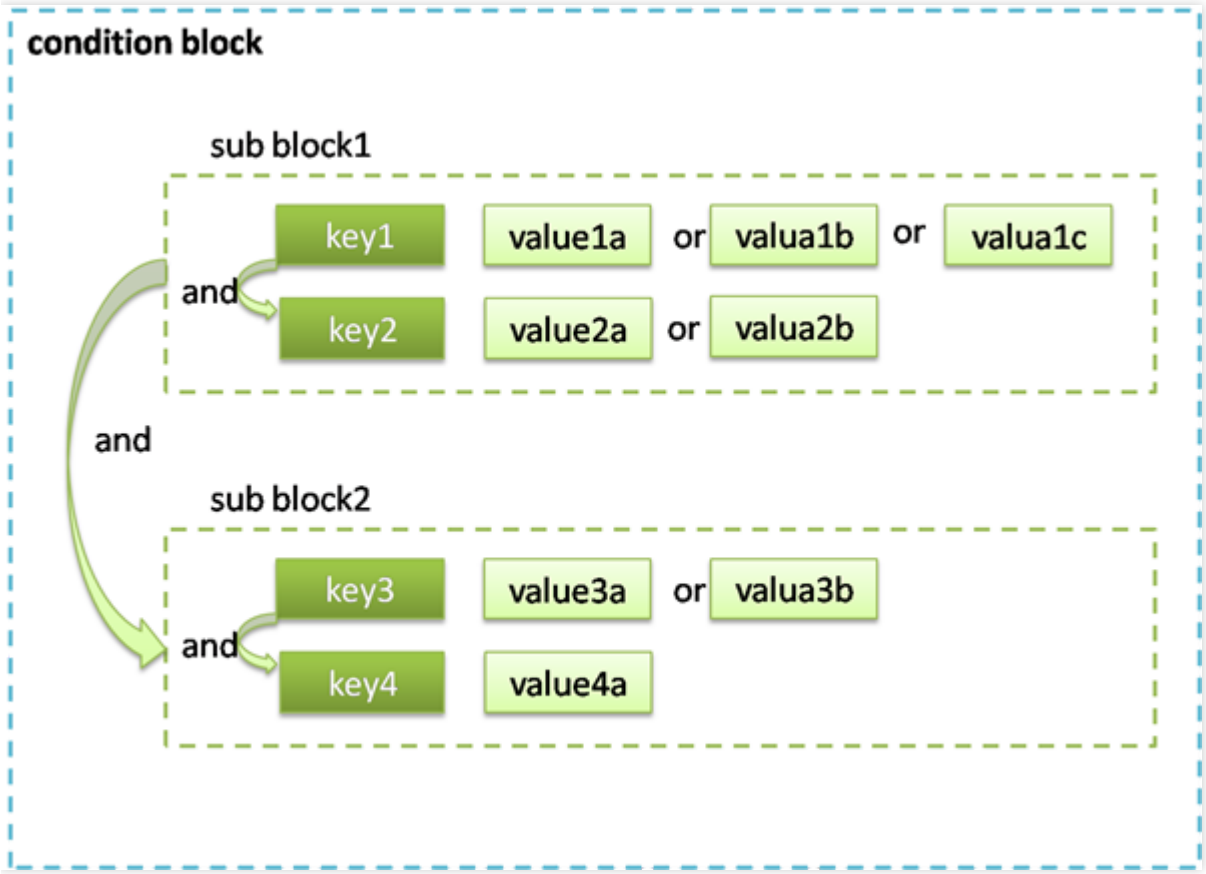
使用场景

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

```
{
 "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"
             ]
         }
     }
 }
}
```

以下示例描述允许 VPC 绑定指定的 NAT 网关， VPC 的地域必须是武汉。

```
{
"version": "2.0",
"statement": {
    "effect": "allow",
    "action": "name/vpc:AcceptVpcPeeringConnection",
    "resource": "qcs::vpc:wh::pcx/2341",
    "condition": {
        "string_equal_if_exist": {
            "vpc:region": "wh"
        }
    }
}
}
```

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”}}

条件操作符	含义	条件名	举例
string_equal_ignore_case	字符串等于(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(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”}}
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”}}

条件操作符	含义	条件名	举例
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}}
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。

版权所有：建行云

排除故障
如何根据故障反馈创建策略

最近更新时间: 2023-09-08 13:50:04

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 CAM 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/0:cvm:wh:uin/10000460####: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。
说明
o 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。
o 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. 参考 [自定义策略关联用户] 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。

版权所有：建行云

企业认证登录管理
接入准备

最近更新时间: 2023-09-08 14:00:22

- 企业方需要提供 cas server
- 云平台的容器网络需要可访问企业 cas sever 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 。

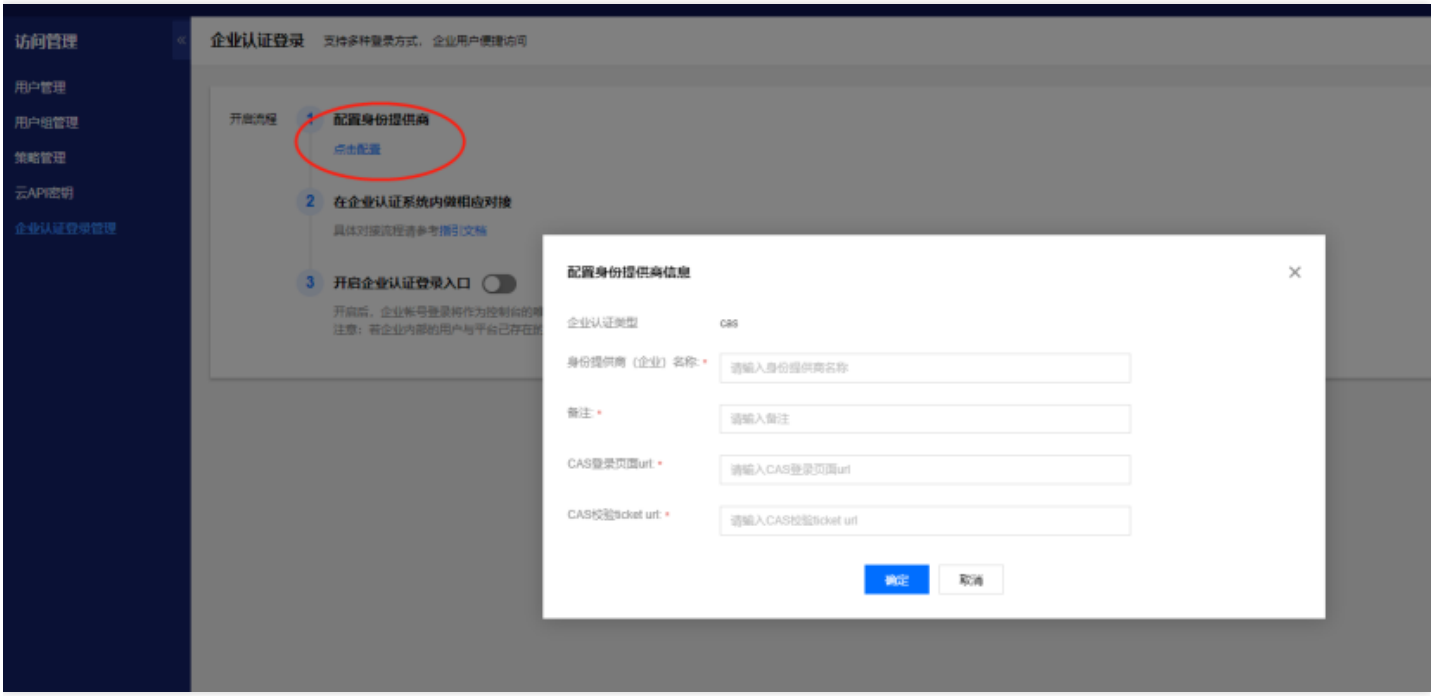
接入步骤

最近更新时间: 2023-09-08 14:00:22

操作步骤

1. 进入建行云租户端控制台 ， 点击【访问管理】>【企业认证登录管理界面】 页面。

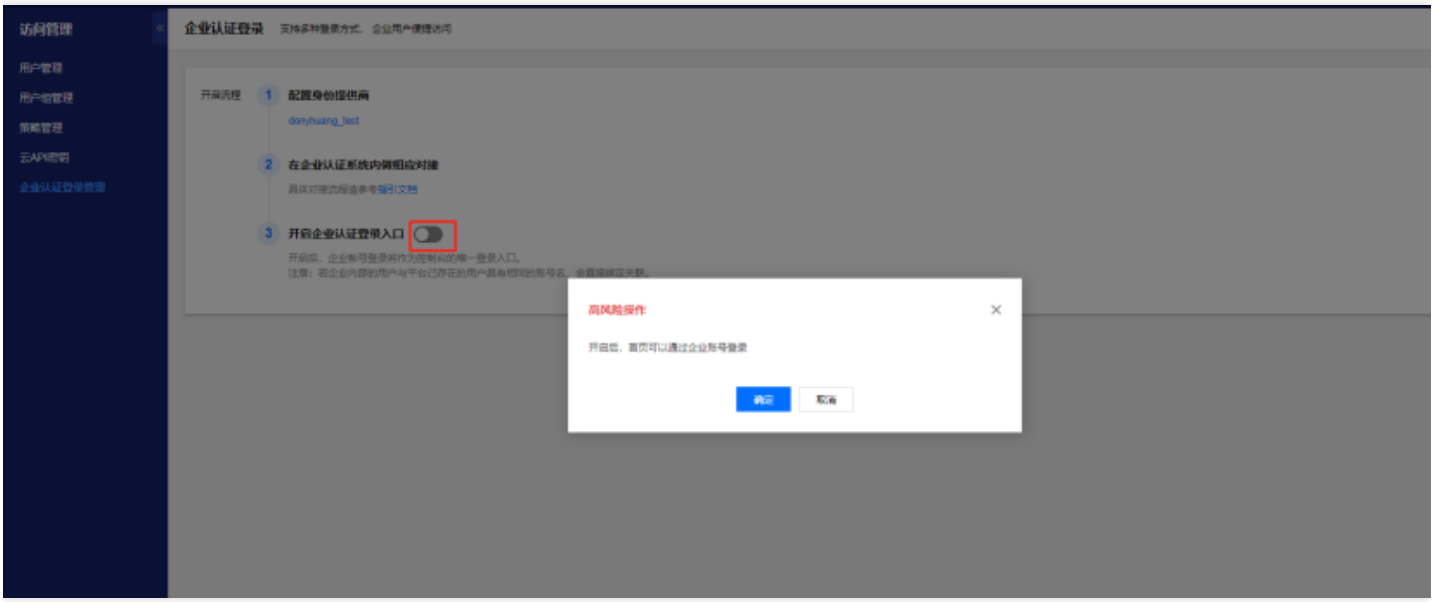
2. 配置企业用户认证CAS相关信息。



3. 配置企业 CAS 登录、校验地址（以上url网络必须与建行云网络可达），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。

版权所有：建行云



5. 企业CAS校验 ticket 返回 xml cas:serviceResponse 必须要求如下字段，否则无法接入成功！

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
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@ccb.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:

请联系建行云平台产品团队做验证。

相关案例

CVM相关案例

最近更新时间: 2023-09-08 14:44:59

授权子账号拥有CVM的所有权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的完全管理权限（创建、管理、云服务器下单支付等全部操作权限）。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMFullAccess、QcloudCVMFinanceAccess授权给子账号Developer。

方案B：

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement":[
        {
            "effect": "allow",
            "action": "cvm:*",
            "resource": "*"
        },
        {
              "effect": "allow",
              "action": "finance:*",
              "resource": "qcs::cvm:::*"
        }
    ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有CVM的只读权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查询CVM实例的权限，但是不具有创建、删除、开关机的权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMInnerReadOnlyAccess授权给子账号Developer。

方案B：

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement":
    {
        "effect": "allow",
        "action": [
                "cvm:Describe*",
                "cvm:Inquiry*"
                ],
        "resource": "*"
    }
}
```

step2：将该策略授权给子账号。

授权子账号拥有CVM相关资源的只读权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查询 CVM 实例及相关资源（VPC 、CLB）的权限，但是不具有创建、删除、开关机的权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMReadOnlyAccess授权给子账号Develope

方案B：

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:Describe*",
                "cvm:Inquiry*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "action": [
                "vpc:Describe*",
                "vpc:Inquiry*",
                "vpc:Get*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "action": [
                "clb:Describe*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "effect": "allow",
            "action": "monitor:*",
            "resource": "*"
        }
    ]
}
```

step2：将该策略授权给子账号。

授权子账号拥有弹性云盘的操作权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查看CVM控制台中的云硬盘信息，创建云硬盘，使用云硬盘的权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCBSFullAccess授权给子账号Developer。

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:CreateCbsStorages",
                "cvm:AttachCbsStorages",
                "cvm:DetachCbsStorages",
                "cvm:ModifyCbsStorageAttributes",
                "cvm:DescribeCbsStorages",
                "cvm:DescribeInstancesCbsNum",
                "cvm:RenewCbsStorage",
                "cvm:ResizeCbsStorage"
                ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。

注：如果不允许子账号修改云硬盘属性，请去掉上述策略语法的”cvm:ModifyCbsStorageAttributes”。

授权子账号拥有安全组的操作权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的查看CVM控制台中的安全组，并且使用安全组的权限。

以下策略允许子账号在CVM 控制台中具有创建，删除安全组的权限。

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:DeleteSecurityGroup",
                "cvm:CreateSecurityGroup"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号

以下策略允许子账号在CVM 控制台中具有创建、删除修改安全组策略的权限。

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:ModifySecurityGroupPolicy",
                "cvm:CreateSecurityGroupPolicy",
                "cvm:DeleteSecurityGroupPolicy"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。

授权子账号拥有弹性IP地址的操作权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查看CVM控制台中的弹性IP地址，并且使用弹性IP地址的权限。

step1：通过策略语法方式创建以下策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:AllocateAddresses",
                "cvm:AssociateAddress",
                "cvm:DescribeAddresses",
                "cvm:DisassociateAddress",
                "cvm:ModifyAddressAttribute",
                "cvm:ReleaseAddresses"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。

以下策略允许子账号查看弹性IP地址并可以将其分配给实例并与之相关联。子账号可以修改弹性IP地址的属性、取消弹性IP地址的关联或释放弹性IP地址。

step1：通过策略语法方式创建以下策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:DescribeAddresses",
                "cvm:AllocateAddresses",
                "cvm:AssociateAddress"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。

授权子账号拥有特定CVM的操作权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的指定CVM机器（id为ins-1,广州地域）的操作权限。

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement": [
        {
            "action": "cvm:*",
            "resource": "qcs::cvm:gz::instance/ins-1",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。

授权子账号拥有特定地域的CVM的操作权限

企业帐号CompanyExample（ownerUin为10000460####）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的武汉地域所有机器的操作权限。

step1：企业帐号CompanyExample直接将预设策略QcloudCVMReadOnlyAccess授权给子账号Developer。

step2：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement": [
        {
            "action": "cvm:*",
            "resource": "qcs::cvm:wh::*",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。