访问管理

产品文档

目录

产品简介
CAM概述

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

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。

应用场景

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

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	1000
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	100
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

> 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

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

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	✓	-	-	-

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
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

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

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

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

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

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

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

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. 在用户情详页中选择安全设置>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

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。

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，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

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

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

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

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。

删除用户组

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

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

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

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。

授权指南
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。

> 说明：
>
> 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。

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/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

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

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

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>)<princi
pal_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 instance
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

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":" ",

策略说明	策略定义
	"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。

1. 有几种描述方式，该字段是必填项。

2. 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>

3. 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>

4. 表示某个资源子类下的所有资源。如 instance/* 。

<resource_type>/*

5. 表示某产品下的所有资源。

*

6. 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。
7. 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。
8. 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

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	qcs:tag	{"string_equal_ignore_case":{"qcs:tag/tag_name1":"tag_value1"}}

条件操作符	含义	条件名	举例
	于(不区分大小写)		
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"}}
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":"2016-06-01T 00:01:00Z"}}
date_less_than_equal	时间小于	qcs:current_time	{" date_less_than ":{"qcs:current_time":"2016-06-01T

条件操作符	含义	条件名	举例
	等于		00:01:00Z"}}
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}}
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

什么是角色

角色可以看作是TCloudFinanceZone的“虚拟账号”，角色同样可被授予策略，拥有在TCloudFinanceZone中允许执行和拒绝执行的权限。角色可以是任一TCloudFinanceZone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

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TCloudFinanceZone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

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

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

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

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

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

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

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。

排除故障
如何根据故障反馈创建策略

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 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/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。 > 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，请将邮箱（cloud_noreply@tencent.com）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

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TCloudFinanceZone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TCloudFinanceZone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
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TCloudFinanceZone集群master节点，进入到 ocloud-tcenter-mc-idplogin pod容器 shell 终端执行：
     a. 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
     b. curl -v http://cas.finance.cloud.tencent.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TCloudFinanceZone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TCloudFinanceZone集群master节点，进入到 ocloud-tcenter-mc-idplogin pod容器 shell 终端执行：
        a. 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
        b. curl -v http://cas.finance.cloud.tencent.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TCloudFinanceZone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

企业微信账号

联合账号

联合账号用来获取企业微信成员账号信息。

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。

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。

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。

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。

4. 点击确定完成配置。

商用案例
CMQ相关案例
授权子帐号拥有消息服务的所有权限

授权子帐号拥有消息服务的所有权限

企业帐号CompanyExample下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample名下的消息队列的所有权限，无论消息队列是主题模型还是队列模型，都可以被读写。

方案A：

企业帐号CompanyExample直接将预设策略QCloudCmqQueueFullAccess和QCloudCmqTopicFullAccess授权给子账号Developer。授权方式请参考授权管理。

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": ["cmqtopic:*","camqueue:*"]
      "resource": "*"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子帐号拥有其创建的消息队列的所有权限

授权子帐号拥有其创建的消息队列的所有权限

企业帐号CompanyExample下有一个子账号Developer，该子账号希望其可以访问自己创建的消息队列。
方案A：
企业帐号CompanyExample直接将预设策略QCloudCmqQueueCreaterFullAccess和QCloudCmqTopicCreaterFullAccess授权给子账号Developer。授权方式请参考授权管理。
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": "cmqtopic:*",
         "resource": "qcs::cmqtopic:::topicName/uin/${uin}/*"
      },
      {
         "effect": "allow",
         "action": "cmqqueue:*",
         "resource": "qcs::cmqqueue:::queueName/uin/${uin}/*"
      }
    ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子帐号拥有特定的主题模型的消息队列的读权限

授权子帐号拥有特定的主题模型的消息队列的读权限

企业帐号CompanyExample（ownerUin为12345678）有一个基于主题模型的消息队列，同时他有一个子账号Developer，希望其可以访问该消息队列。
step1：通过策略语法方式创建以下策略：

```
{
    "version": "2.0",
    "statement":
    {
        "action": "cmqqueue:SendMessage",
        "resource":"qcs::cmqqueue:::queueName/uin/12345678/test-caten",
        "effect": "allow"
    }
}
```

step2：将该策略授权给子账号。

CVM相关案例
授权子账号拥有CVM的所有权限

授权子账号拥有CVM的所有权限

企业帐号CompanyExample（ownerUin为12345678）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

授权子账号拥有CVM的只读权限

企业帐号CompanyExample（ownerUin为12345678）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

授权子账号拥有CVM相关资源的只读权限

企业帐号CompanyExample（ownerUin为12345678）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

授权子账号拥有弹性云盘的操作权限

企业帐号CompanyExample（ownerUin为12345678）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

授权子账号拥有安全组的操作权限

企业帐号CompanyExample（ownerUin为12345678）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

授权子账号拥有弹性IP地址的操作权限

企业帐号CompanyExample（ownerUin为12345678）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。/64296768352841728/64296770256007168。

授权子账号拥有特定CVM的操作权限

授权子账号拥有特定CVM的操作权限

企业帐号CompanyExample（ownerUin为12345678）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

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12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的广州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:gz::*",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。

授权子账号拥有CVM的所有权限但不包括支付权限

授权子账号拥有CVM的所有权限但不包括支付权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的所有权限管理权限（创建、管理等全部操作），但不包括支付权限，可以下单但无法支付。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMFullAccess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": "*"
      }
  ]
}
```

step2：将该策略授权给子账号。

授予子账号不支持项目的产品的查看权限

案例场景

企业账号 CompanyExample（ownerUin为12345678）下有一个子账号 Developer，需要授权子账号在控制台查看快照、镜像、VPC、弹性公网 IP 等产品。

操作指引

授权子账号 QcloudCVMAccessForNullProject 预设策略。

故障处理
故障处理

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cam-sts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cam-security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-grant-write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（cloudoreply@tencent.com）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。

API文档
访问管理（cam）
版本（2019-01-16）
API 概览

API版本

V3

其他接口

接口名称	接口功能
AttachRolePolicies	绑定多个策略到角色
AttachRolePolicy	绑定权限策略到角色
AttachRolesPolicy	绑定多个角色到策略
CreatePolicy	创建策略
CreateRole	创建角色
DeletePolicy	删除策略
DeleteRole	删除角色
DescribeRoleList	获取角色列表
DetachGroupPolicies	解除绑定多个策略到用户组
DetachGroupsPolicy	解除绑定策略到多个用户组
DetachUsersPolicy	解除绑定策略到多个用户
GetPolicy	查看策略详情
GetRole	获取角色详情
GetServiceRoleInfo	获取服务角色信息

接口名称	接口功能
ListAttachedGroupPolicies	查询用户组关联的策略列表
ListAttachedRolePolicies	获取角色绑定的策略列表
ListEntitiesForPolicy	查询策略关联的实体列表
ListPolicies	查询策略列表
UpdateAssumeRolePolicy	修改角色信任策略
UpdatePolicy	更新策略

用户相关接口

接口名称	接口功能
GetPasswordRules	获取CAM密码规则
GetSubsGroup	子账户所属用户组列表
GetUinBySecretId	根据SecretId查询Uin
UpdatePasswordRules	更新CAM密码规则

身份提供商接口

接口名称	接口功能
CreateOauthProvider	新增oauth配置
GetUserAccessToken	获取用户oauth标识
RefreshUserToken	刷新用户userAccessToken
UpdateOauthProvider	更新Oauth配置信息
VerifyUserAccessToken	验证用户userAccessToken

调用方式
接口签名v1

TCloudFinanceZone API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（ Signature ）以验证请求者身份。
签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。
安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录TCloudFinanceZone管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. 生成签名串

有了安全凭证SecretId 和 SecretKey后，就可以生成签名串了。以下是生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

注意：这里只是示例，请根据用户实际申请的 SecretId 和 SecretKey 进行后续操作！

以云服务器查看实例列表(DescribeInstances)请求为例，当用户调用这一接口时，其请求参数可能如下:

参数名称	中文	参数值

参数名称	中文	参数值
Action	方法名	DescribeInstances
SecretId	密钥Id	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	shjr
InstanceIds.0	待查询的实例ID	ins-09dx96dg
Offset	偏移量	0
Limit	最大允许输出	20
Version	接口版本号	2017-03-12

2.1. 对参数排序

首先对所有请求参数按参数名的字典序（ ASCII 码）升序排序。注意：1）只按参数名进行排序，参数值保持对应即可，不参与比大小；2）按 ASCII 码比大小，如 InstanceIds.2 要排在 InstanceIds.12 后面，不是按字母表，也不是按数值。用户可以借助编程语言中的相关排序函数来实现这一功能，如 php 中的 ksort 函数。上述示例参数的排序结果如下:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'shjr',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

使用其它程序设计语言开发时，可对上面示例中的参数进行排序，得到的结果一致即可。

2.2. 拼接请求字符串

此步骤生成请求字符串。
将把上一步排序好的请求参数格式化成“参数名称”=“参数值”的形式，如对 Action 参数，其参数名称为 "Action" ，参数值为 "DescribeInstances" ，因此格式化后就为 Action=DescribeInstances 。
注意：“参数值”为原始值而非url编码后的值。

然后将格式化后的各个参数用"&"拼接在一起，最终生成的请求字符串为:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. 拼接签名原文字符串

此步骤生成签名原文字符串。
签名原文字符串由以下几个参数构成:

1. 请求方法: 支持 POST 和 GET 方式，这里使用 GET 请求，注意方法为全大写。
2. 请求主机:查看实例列表(DescribeInstances)的请求域名为：cvm.finance.cloud.tencent.com。实际的请求域名根据接口所属模块的不同而不同，详见各接口说明。
3. 请求路径: 当前版本云API的请求路径固定为 / 。
4. 请求字符串: 即上一步生成的请求字符串。

签名原文串的拼接规则为: 请求方法 + 请求主机 +请求路径 + ? + 请求字符串

示例的拼接结果为：

```
GETcvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. 生成签名串

此步骤生成签名串。
首先使用 HMAC-SHA1 算法对上一步中获得的签名原文字符串进行签名，然后将生成的签名串使用 Base64 进行编码，即可获得最终的签名串。

具体代码如下，以 PHP 语言为例:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

最终得到的签名串为:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

使用其它程序设计语言开发时，可用上面示例中的原文进行签名验证，得到的签名串与例子中的一致即可。

3. 签名串编码

生成的签名串并不能直接作为请求参数，需要对其进行 URL 编码。

如上一步生成的签名串为 EliP9YW3pW28FpsEdkXt/+WcGeI= ，最终得到的签名串请求参数（Signature）为：EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d，它将用于生成最终的请求 URL。

注意：如果用户的请求方法是 GET，或者请求方法为 POST 同时 Content-Type 为 application/x-www-form-urlencoded，则发送请求时所有请求参数的值均需要做 URL 编码，参数键和=符号不需要编码。非 ASCII 字符在 URL 编码前需要先以 UTF-8 进行编码。

注意：有些编程语言的 http 库会自动为所有参数进行 urlencode，在这种情况下，就不需要对签名串进行 URL 编码了，否则两次 URL 编码会导致签名失败。

注意：其他参数值也需要进行编码，编码采用 RFC 3986。使用 %XY 对特殊字符例如汉字进行百分比编码，其中“X”和“Y”为十六进制字符（0-9 和大写字母 A-F），使用小写将引发错误。

4. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

5. 签名演示

在实际调用 API 3.0 时，推荐使用配套的TCloudFinanceZone SDK 3.0 ，SDK 封装了签名的过程，开发时只关注产品提供的具体接口即可。详细信息参见 SDK 中心。当前支持的编程语言有：

- Python
- Java

- PHP
- Go
- Node

为了更清楚的解释签名过程，下面以实际编程语言为例，将上述的签名过程具体实现。请求的域名、调用的接口和参数的取值都以上述签名过程为准，代码只为解释签名过程，并不具备通用性，实际开发请尽量使用 SDK 。

最终输出的 url 可能为： https://cvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

注意：由于示例中的密钥是虚构的，时间戳也不是系统当前时间，因此如果将此 url 在浏览器中打开或者用 curl 等命令调用时会返回鉴权错误：签名过期。为了得到一个可以正常返回的 url ，需要修改示例中的 SecretId 和 SecretKey 为真实的密钥，并使用系统当前时间戳作为 Timestamp 。

注意：在下面的示例中，不同编程语言，甚至同一语言每次执行得到的 url 可能都有所不同，表现为参数的顺序不同，但这并不影响正确性。只要所有参数都在，且签名计算正确即可。

注意：以下代码仅适用于 API 3.0，不能直接用于其他的签名流程，即使是旧版的 API ，由于存在细节差异也会导致签名计算错误，请以对应的实际文档为准。

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.finance.cloud.tencent.com/?");
```

```
        // 签名时要求对参数进行字典排序，此处用TreeMap保证顺序
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.finance.cloud.tencent.com/?");
        // 实际请求的url中对参数顺序没有要求
        for (String k : params.keySet()) {
            // 需要对请求串进行urlencode，由于key都是英文字母，故此处仅对其value进行urlencode
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap可以自动排序
        // 实际调用时应当使用随机数，例如：params.put("Nonce", new Random().nextInt(java.lang.Intege
r.MAX_VALUE));
        params.put("Nonce", 11886); // 公共参数
        // 实际调用时应当使用系统当前时间，例如：  params.put("Timestamp", System.currentTimeMillis() /
1000);
        params.put("Timestamp", 1465185768); // 公共参数
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // 公共参数
        params.put("Action", "DescribeInstances"); // 公共参数
        params.put("Version", "2017-03-12"); // 公共参数
        params.put("Region", "shjr"); // 公共参数
        params.put("Limit", 20); // 业务参数
        params.put("Offset", 0); // 业务参数
        params.put("InstanceIds.0", "ins-09dx96dg"); // 业务参数
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // 公共参数
        System.out.println(getUrl(params));
    }
}
```

Python

注意：如果是在 Python 2 环境中运行，需要先安装 requests 依赖包： pip install requests 。

```
# -*- coding: utf8 -*-
import base64
```

```
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.finance.cloud.tencent.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'shjr',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # 此处会实际调用，成功后可能产生计费
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

接口签名v3

TCloudFinanceZone API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。
签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。
安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录TCloudFinanceZone管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. TC3-HMAC-SHA256 签名方法

注意：对于GET方法，只支持 Content-Type: application/x-www-form-urlencoded 协议格式。对于POST方法，目前支持 Content-Type: application/json 以及 Content-Type: multipart/form-data 两种协议格式，json 格式默认所有业务接口均支持，multipart 格式只有特定业务接口支持，此时该接口不能使用 json 格式调用，参考具体业务接口文档说明。

下面以云服务器查询广州区实例列表作为例子，分步骤介绍签名的计算过程。我们仅用到了查询实例列表的两个参数：Limit 和 Offset，使用 GET 方法调用。

假设用户的 SecretId 和 SecretKey 分别是：AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 和 Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

2.1. 拼接规范请求串

按如下格式拼接规范请求串（CanonicalRequest）：

```
CanonicalRequest =
    HTTPRequestMethod + '\n' +
    CanonicalURI + '\n' +
    CanonicalQueryString + '\n' +
    CanonicalHeaders + '\n' +
    SignedHeaders + '\n' +
    HashedRequestPayload
```

- HTTPRequestMethod：HTTP 请求方法（GET、POST ），本示例中为 GET；
- CanonicalURI：URI 参数，API 3.0 固定为正斜杠（/）；
- CanonicalQueryString：发起 HTTP 请求 URL 中的查询字符串，对于 POST 请求，固定为空字符串，对于 GET 请求，则为 URL 中问号（?）后面的字符串内容，本示例取值为：Limit=10&Offset=0。注意：CanonicalQueryString 需要经过 URL 编码。
- CanonicalHeaders：参与签名的头部信息，至少包含 host 和 content-type 两个头部，也可加入自定义的头部参与签名以提高自身请求的唯一性和安全性。拼接规则：1）头部 key 和 value 统一转成小写，并去掉首尾空格，按照 key:value\n 格式拼接；2）多个头部，按照头部 key（小写）的字典排序进行拼接。此例中为： content-type:application/x-www-form-urlencoded\nhost:cvm.finance.cloud.tencent.com\n
- SignedHeaders：参与签名的头部信息，说明此次请求有哪些头部参与了签名，和 CanonicalHeaders 包含的头部内容是一一对应的。content-type 和 host 为必选头部。拼接规则：1）头部 key 统一转成小写；2）多个头部 key（小写）按照字典排序进行拼接，并且以分号（;）分隔。此例中为： content-type;host
- HashedRequestPayload：请求正文的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(RequestPayload)))，对 HTTP 请求整个正文 payload 做 SHA256 哈希，然后十六进制编码，最后编码串转换成小写字母。注意：对于 GET 请求，RequestPayload 固定为空字符串，对于 POST 请求，RequestPayload 即为 HTTP 请求正文 payload。

根据以上规则，示例中得到的规范请求串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
GET
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.finance.cloud.tencent.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. 拼接待签名字符串

按如下格式拼接待签名字符串：

```
StringToSign =
    Algorithm + \n +
```

```
RequestTimestamp + \n +
CredentialScope + \n +
HashedCanonicalRequest
```

- Algorithm：签名算法，目前固定为 TC3-HMAC-SHA256；
- RequestTimestamp：请求时间戳，即请求头部的 X-TC-Timestamp 取值，如上示例请求为 1539084154；
- CredentialScope：凭证范围，格式为 Date/service/tc3_request，包含日期、所请求的服务和终止字符串（tc3_request）。Date 为 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service 为产品名，必须与调用的产品域名一致，例如 cvm。如上示例请求，取值为 2018-10-09/cvm/tc3_request；
- HashedCanonicalRequest：前述步骤拼接所得规范请求串的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))。

注意：

> 1. Date 必须从时间戳 X-TC-Timestamp 计算得到，且时区为 UTC+0。如果加入系统本地时区信息，例如东八区，将导致白天和晚上调用成功，但是凌晨时调用必定失败。假设时间戳为 1551113065，在东八区的时间是 2019-02-26 00:44:25，但是计算得到的 Date 取 UTC+0 的日期应为 2019-02-25，而不是 2019-02-26。
> 2. Timestamp 必须是当前系统时间，且需确保系统时间和标准时间是同步的，如果相差超过五分钟则必定失败。如果长时间不和标准时间同步，可能导致运行一段时间后，请求必定失败（返回签名过期错误）。

根据以上规则，示例中得到的待签名字符串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. 计算签名

1）计算派生签名密钥，伪代码如下

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey：原始的 SecretKey；
- Date：即 Credential 中的 Date 字段信息，如上示例，为2018-10-09；
- Service：即 Credential 中的 Service 字段信息，如上示例，为 cvm；

2）计算签名，伪代码如下

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning：即以上计算得到的派生签名密钥；
- StringToSign：即步骤2计算得到的待签名字符串；

2.4. 拼接 Authorization

按如下格式拼接 Authorization：

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm：签名方法，固定为 TC3-HMAC-SHA256；
- SecretId：密钥对中的 SecretId；
- CredentialScope：见上文，凭证范围；
- SignedHeaders：见上文，参与签名的头部信息；
- Signature：签名值

根据以上规则，示例中得到的值为：

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

最终完整的调用信息如下：

```
https://cvm.finance.cloud.tencent.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.finance.cloud.tencent.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: shjr
```

3. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

4. 签名演示

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.finance.cloud.tencent.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
```

```
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.finance.cloud.tencent.com";
        String region = "shjr";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // 注意时区，否则容易出错
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* 步骤 1：拼接规范请求串 *************
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* 步骤 2：拼接待签名字符串 *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* 步骤 3：计算签名 *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
```

```
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* 步骤 4：拼接 Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# 密钥参数
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.finance.cloud.tencent.com"
endpoint = "https://" + host
region = "shjr"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* 步骤 1：拼接规范请求串 *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
```

```
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* 步骤 2：拼接待签名字符串 *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)

# ************* 步骤 3：计算签名 *************
# 计算签名摘要函数
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* 步骤 4：拼接 Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# 公共参数添加到请求头部
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
```

```
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

请求结构

1. 服务地址

地域（Region）是指物理的数据中心的地理区域。TCloudFinanceZone交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 查询地域列表 查看完成的地域列表。

2. 通信协议

TCloudFinanceZone API 的所有接口均通过 HTTPS 进行通信，提供高安全性的通信通道。

3. 请求方法

支持的 HTTP 请求方法:

- POST（推荐）
- GET

POST 请求支持的 Content-Type 类型：

- application/json（推荐），必须使用 TC3-HMAC-SHA256 签名方法。
- application/x-www-form-urlencoded，必须使用 HmacSHA1 或 HmacSHA256 签名方法。
- multipart/form-data（仅部分接口支持），必须使用 TC3-HMAC-SHA256 签名方法。

GET 请求的请求包大小不得超过 32 KB。POST 请求使用签名方法为 HmacSHA1、HmacSHA256 时不得超过 1 MB。POST 请求使用签名方法为 TC3-HMAC-SHA256 时支持 10 MB。

4. 字符编码

均使用UTF-8编码。

返回结果

正确返回结果

以云服务器的接口查看实例状态列表 (DescribeInstancesStatus) 2017-03-12 版本为例，若调用成功，其可能的返回如下为：

```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```

- Response 及其内部的 RequestId 是固定的字段，无论请求成功与否，只要 API 处理了，则必定会返回。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。
- 除了固定的字段外，其余均为具体接口定义的字段，不同的接口所返回的字段参见接口文档中的定义。此例中的 TotalCount 和 InstanceStatusSet 均为 DescribeInstancesStatus 接口定义的字段，由于调用请求的用户暂时还没有云服务器实例，因此 TotalCount 在此情况下的返回值为 0， InstanceStatusSet 列表为空。

错误返回结果

若调用失败，其返回值示例如下为：

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

- Error 的出现代表着该请求调用失败。Error 字段连同其内部的 Code 和 Message 字段在调用失败时是必定返回的。
- Code 表示具体出错的错误码，当请求出错时可以先根据该错误码在公共错误码和当前接口对应的错误码列表里面查找对应原因和解决方案。

- Message 显示出了这个错误发生的具体原因，随着业务发展或体验优化，此文本可能会经常保持变更或更新，用户不应依赖这个返回值。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。

公共错误码

返回结果中如果存在 Error 字段，则表示调用 API 接口失败。 Error 中的 Code 字段表示错误码，所有业务都可能出现的错误码为公共错误码，下表列出了公共错误码。

错误码	错误描述
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。
AuthFailure.SignatureExpire	签名过期。
AuthFailure.SignatureFailure	签名错误。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。

错误码	错误描述
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

公共参数

公共参数是用于标识用户和接口鉴权目的的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

签名方法 v3

使用 TC3-HMAC-SHA256 签名方法时，公共参数需要统一放到 HTTP Header 请求头部中，如下：

参数名称	类型	必选	描述
X-TC-Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
X-TC-Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
X-TC-Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如 1529223702。注意：如果与服务器时间相差超过5分钟，会引起签名过期错误。
X-TC-Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
Authorization	String	是	HTTP 标准身份认证头部字段，例如： TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 其中， - TC3-HMAC-SHA256：签名方法，目前固定取该值； - Credential：签名凭证，AKIDEXAMPLE 是 SecretId；Date 是 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service为产品名，必须与调用的产品域名一致，例如cvm； - SignedHeaders：参与签名计算的头部信息，content-type 和 host 为必选头部； - Signature：签名摘要。
X-TC-Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token。

签名方法 v1

使用 HmacSHA1 和 HmacSHA256 签名方法时，公共参数需要统一放到请求串中，如下

参数名称	类型	必选	描述
Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。

参数名称	类型	必选	描述
Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如1529223702，如果与当前时间相差过大，会引起签名过期错误。
Nonce	Integer	是	随机正整数，与 Timestamp 联合起来，用于防止重放攻击。
SecretId	String	是	在云API密钥上申请的标识身份的 SecretId，一个 SecretId 对应唯一的 SecretKey ，而 SecretKey 会用来生成请求签名 Signature。
Signature	String	是	请求签名，用来验证此次请求的合法性，需要用户根据实际的输入参数计算得出。具体计算方法参见接口鉴权文档。
Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
SignatureMethod	String	否	签名方式，目前支持 HmacSHA256 和 HmacSHA1。只有指定此参数为 HmacSHA256 时，才使用 HmacSHA256 算法验证签名，其他情况均使用 HmacSHA1 验证签名。
Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token 。

地域列表

地域（Region）是指物理的数据中心的地理区域。TCloudFinanceZone交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 查询地域列表 查看完成的地域列表。

其他接口
绑定多个策略到角色

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

绑定多个策略到角色

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:02:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AttachRolePolicies
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleId	否	否	Uint64	角色ID(与角色名称必传一项) 示例值： 4611686018427387904
RoleName	否	否	String	角色名称(与角色ID必传一项) 示例值： QCS_RoleName
PolicyId	否	否	Array of Uint64	策略ID list(与策略名 list必传一项) 示例值： [1001,1002]
PolicyName	否	否	Array of String	策略名 list(与策略ID list必传一项) 示例值： ["policygen-1","policygen-2"]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation.PolicyFull	用户策略数超过上限。
InvalidParameter.OperatePoliciesOverLimit	一次操作策略数过多。
InvalidParameter.PasswordLengthTooShort	密码太短。
InternalError.SystemError	内部错误。
InvalidParameter.ParamError	非法入参。
InvalidParameter.PolicyIdNotExist	策略ID不存在。

绑定权限策略到角色

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（AttachRolePolicy）用于绑定策略到角色。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:02:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AttachRolePolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	否	否	Uint64	策略ID，入参PolicyId与PolicyName二选一 示例值： 1
AttachRoleId	否	否	String	角色ID，用于指定角色，入 参 AttachRoleId 与 AttachRoleName 二选一 示例值： 4611686018427397905
AttachRoleName	否	否	String	角色名称，用于指定角色，入 参 AttachRoleId 与 AttachRoleName 二选一 示例值： QCS_RoleName
PolicyName	否	否	String	策略名，入参PolicyId与PolicyName二选一 示例值： policygen-20141112201913

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.PolicyIdNotExist	策略ID不存在。
InternalError.SystemError	内部错误。
InvalidParameter.RoleNotExist	角色不存在。
InvalidParameter.AttachmentFull	principal字段的授权对象关联策略数已达到上限。

绑定多个角色到策略

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

绑定多个角色到策略

默认接口请求频率限制：20次/秒。

接口更新时间：2023-02-09 15:36:51。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AttachRolesPolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleId	否	否	Array of Uint64	角色ID(与角色名称必传一项) 示例值： [4611686018427387904,4611686018427387905]
RoleName	否	否	Array of String	角色名称(与角色ID必传一项) 示例值： ["role-1","role-2"]
PolicyId	否	否	Uint64	策略ID(与策略名必传一项) 示例值： 1000
PolicyName	否	否	String	策略名(与策略ID必传一项) 示例值： policygen-20141112201913

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation.PolicyFull	用户策略数超过上限。
InvalidParameter.OperatePoliciesOverLimit	一次操作策略数过多。
InvalidParameter.PasswordLengthTooShort	密码太短。
InternalError.SystemError	内部错误。
InvalidParameter.ParamError	非法入参。
InvalidParameter.PolicyIdNotExist	策略ID不存在。

创建策略

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（CreatePolicy）可用于创建策略。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-02 16:17:55。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreatePolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyName	是	否	String	策略名 示例值： policygen-20141112201913
Description	否	否	String	策略描述 示例值： 测试描述信息
PolicyDocument	是	否	String	策略文档，示例：{"version":"2.0","statement":[{"action":"name/sts:AssumeRole","effect":"allow","principal":{"service":["cloudaudit.<no value>","cls.<no value>"]}}]}，principal用于指定角色的授权对象。获取该参数可参阅 获取角色详情（https://<no value>/document/product/598/36221）输出参数RoleInfo 示例值： {"version":"2.0","statement":[{"effect":"allow","action":"cvm:Describe*","resource":"*"}]}
CreateMode	否	否	Uint64	创建模式，1 dbsql带出来的预设策略, 2 按策略模版创建 角色策略 COS侧后台接口创建, 3 按照策略生成器创建, 4 标签相关 示例值： 1

3. 输出参数

参数名称	类型	描述
PolicyId	Uint64	策略id 示例值： 1000
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
ResourceNotFound.UserNotExist	用户不存在。
FailedOperation.PolicyFull	用户策略数超过上限。
InternalError.SystemError	内部错误。
InvalidParameter.ActionNotExist	action不存在

创建角色

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（CreateRole）用于创建角色。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:02:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateRole
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleName	是	否	String	角色名称 示例值： QCS
PolicyDocument	是	否	String	策略文档，示例：{"version":"2.0","statement":[{"action":"name/sts:AssumeRole","effect":"allow","principal":{"service":["cloudaudit.<no value>","cls.<no value>"]}}]}，principal用于指定角色的授权对象。获取该参数可参阅 获取角色详情（https://<no value>/document/product/598/36221）输出参数RoleInfo 示例值： {"version":"2.0","statement":[{"action":"sts:AssumeRole","effect":"allow","principal":{"qcs":["qcs::cam::uin/110000000007:root"]}}]}
Description	否	否	String	角色描述 示例值： adesc
ConsoleLogin	否	否	Uint64	是否允许登录 1 为允许 0 为不允许 示例值： 0

参数名称	必选	允许NULL	类型	描述
SessionDuration	否	否	Uint64	申请角色临时密钥的最长有效期限制(范围：0~43200) 示例值： 3600
RoleType	否	否	String	角色类型(system

3. 输出参数

参数名称	类型	描述
RoleId	String	角色ID 示例值： 4611686018427388476
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.AttachmentFull	principal字段的授权对象关联策略数已达到上限。
InvalidParameter.ConditionError	策略文档的condition字段不合法。
InvalidParameter.DescriptionLengthOverlimit	Description入参长度不能大于300字节。
InvalidParameter.PrincipalError	策略文档的principal字段不合法。
InvalidParameter.RoleFull	角色数量达到上限。
InvalidParameter.RoleNameError	角色名不合法。
InvalidParameter.RoleNameInUse	相同名称的角色已存在。
InvalidParameter.UserNotExist	用户对象不存在。
InternalError.SystemError	内部错误。
InvalidParameter.ParamError	非法入参。

删除策略

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

删除策略

默认接口请求频率限制：20次/秒。

接口更新时间：2024-11-11 16:48:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeletePolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	否	否	Array of Uint64	数组，数组成员是策略 id，支持批量删除策略 示例值： [1000,1001]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError.SystemError	内部错误。
InvalidParameter.ParamError	非法入参。
InvalidParameter.PolicyIdError	输入参数PolicyId不合法。
InvalidParameter.PolicyIdNotExist	策略ID不存在。
ResourceNotFound.NotFound	资源不存在。
ResourceNotFound.PolicyIdNotFound	PolicyId指定的资源不存在。

删除角色

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（DeleteRole）用于删除指定角色。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:02:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteRole
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleId	否	否	String	角色ID，用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： 4611686018427844696
RoleName	否	否	String	角色名称，用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： QCS_RoleName

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError.SystemError	内部错误。
InvalidParameter.RoleNotExist	角色不存在。
InvalidParameter.ParamError	非法入参。

获取角色列表

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（DescribeRoleList）用于获取账号下的角色列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-02 21:20:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRoleList
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Page	是	否	Uint64	页码，从1开始 示例值： 1
Rp	是	否	Uint64	每页行数，不能大于200 示例值： 5
Service	否	否	String	按角色的服务账号载体过滤 示例值： cvm
Keyword	否	否	Array of String	按角色名或角色描述过滤 示例值： ["rolename","roleid"]

3. 输出参数

参数名称	类型	描述
List	Array of	角色详情列表。

参数名称	类型	描述
	RoleInfo	示例值：查看
TotalNum	Uint64	角色总数 示例值： 14
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError.SystemError	内部错误。
InvalidParameter.ParamError	非法入参。

解除绑定多个策略到用户组

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

解除绑定多个策略到用户组

默认接口请求频率限制：20次/秒。

接口更新时间：2024-11-11 16:49:40。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DetachGroupPolicies
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
GroupId	是	否	Uint64	用户组ID 示例值： 1000
PolicyId	是	否	Array of Uint64	策略ID list 示例值： [1000,1001]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
InvalidParameter.PolicyIdNotExist	策略ID不存在。
InternalError.SystemError	内部错误。
InvalidParameter.PolicyIdError	输入参数PolicyId不合法。

解除绑定策略到多个用户组

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

解除绑定策略到多个用户组

默认接口请求频率限制：20次/秒。

接口更新时间：2024-11-11 16:50:02。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DetachGroupsPolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
GroupId	是	否	Array of Uint64	用户组ID list 示例值： [1000,1001]
PolicyId	是	否	Uint64	策略ID 示例值： 1000

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
InvalidParameter.PolicyIdNotExist	策略ID不存在。
InternalError.SystemError	内部错误。
InvalidParameter.PolicyIdError	输入参数PolicyId不合法。

解除绑定策略到多个用户

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

解除绑定策略到多个用户

默认接口请求频率限制：20次/秒。

接口更新时间：2024-11-11 16:51:47。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DetachUsersPolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TargetUin	是	否	Array of Uint64	目标用户ID list 示例值： [1000,1001]
PolicyId	是	否	Uint64	策略ID 示例值： 1000

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
InvalidParameter.PolicyIdNotExist	策略ID不存在。
FailedOperation.PolicyFull	用户策略数超过上限。
InternalError.SystemError	内部错误。

查看策略详情

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（GetPolicy）可用于查询查看策略详情。

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-02 21:20:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：GetPolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	是	否	Uint64	策略Id 示例值： 17698703

3. 输出参数

参数名称	类型	描述
PolicyName	String	策略名 示例值： policygen-20141112201913
Description	String	策略描述 示例值： 测试策略
Type	Uint64	1 表示自定义策略，2 表示预设策略 示例值： 1

参数名称	类型	描述
AddTime	Datetime	创建时间 示例值： 2019-04-29 21:18:28
UpdateTime	Datetime	最近更新时间 示例值： 2019-04-29 21:28:32
PolicyDocument	String	策略文档 示例值： {"version":"2.0","statement":[{"effect":"allow","action":["name\/cos:*"],"resource":["*"]}]}
PresetAlias	String	备注 示例值： 备注
IsServiceLinkedRolePolicy	Uint64	是否服务相关策略 示例值： 1
CreateMode	Uint64	1 dbsql带出来的预设策略, 2 按策略模版创建 角色策略 COS侧后台接口创建, 3 按照策略生成器创建, 4 标签相关 示例值： 1
IsCheck	Uint64	秘钥是否验证 1、已验证 0未验证 示例值： 1
PolicyId	Uint64	策略 ID 示例值： 1000
ServiceType	String	服务名称 示例值： cvm
Attachments	Uint64	关联的用户数 示例值： 1
IsAttached	Uint64	当需要查询标记实体是否已经关联策略时不为null。0表示未关联策略，1表示已关联策略 示例值： 1
Deactived	Uint64	是否已下线，传1代表已下线，传0代表未下线 示例值： 0
DeactivedDetail	Array of String	已下线产品列表 示例值： ["deacproduct"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceNotFound.PolicyIdNotFound	PolicyId指定的资源不存在。
InvalidParameter.ParamError	非法入参。
InternalError.SystemError	内部错误。
InvalidParameter.PolicyIdError	输入参数PolicyId不合法。

获取角色详情

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（GetRole）用于获取指定角色的详细信息。

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-02 21:20:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：GetRole
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleId	否	否	String	角色 ID，用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： 4611686018427844696
RoleName	否	否	String	角色名，用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： QCSRole

3. 输出参数

参数名称	类型	描述
RoleInfo	RoleInfo	角色详情 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError.SystemError	内部错误。
InvalidParameter.ParamError	非法入参。
InvalidParameter.RoleNotExist	角色不存在。

获取服务角色信息

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

获取服务角色信息

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-02 21:20:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：GetServiceRoleInfo
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleName	否	否	String	角色名 示例值： QCS
PolicyName	否	否	Array of String	策略名列表 示例值： ["policygen-1","policygen-2"]

3. 输出参数

参数名称	类型	描述
RoleName	String	角色名 示例值： QCS
ServiceType	String	业务类型 示例值： cvm

参数名称	类型	描述
ServiceTypeEn	String	英文业务类型 示例值： cvm
RoleDesc	String	角色描述 示例值： QCS
RoleDescEn	String	角色英文描述 示例值： QCS
PolicyName	String	预设策略名 示例值： policygen-20141112201913
Remark	String	描述 示例值： remark
EnRemark	String	英文描述 示例值： ""
PolicyList	Array of RolePolicyList	策略列表 示例值：查看
RoleDescI18n	String	支持国际化的角色描述 示例值： ""
Id	String	角色Id 示例值： ""
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
InternalError.SystemError	内部错误。

查询用户组关联的策略列表

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

查询用户组关联的策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-02 21:20:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ListAttachedGroupPolicies
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
TargetGroupId	是	否	Uint64	用户组ID 示例值： 3349
Page	是	否	Uint64	页码，默认值是 1，从 1 开始 示例值： 1
Rp	是	否	Uint64	每页大小，默认值是 20 示例值： 10

3. 输出参数

参数名称	类型	描述
TotalNum	Uint64	策略总数 示例值： 1

参数名称	类型	描述
List	Array of AttachPolicyInfo	策略列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
InternalError.SystemError	内部错误。

获取角色绑定的策略列表

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（ListAttachedRolePolicies）用于获取角色绑定的策略列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-02 21:20:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ListAttachedRolePolicies
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleId	否	否	String	角色 ID。用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： 4611686018427397905
RoleName	否	否	String	角色名。用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： role_data
PolicyType	否	否	String	按策略类型过滤，User表示仅查询自定义策略，QCS表示仅查询预设策略 示例值： 1
Page	是	否	Uint64	页码，从 1 开始 示例值： 1
Rp	是	否	Uint64	每页行数，不能大于200 示例值： 10

3. 输出参数

参数名称	类型	描述
List	Array of AttachedPolicyOfRole	角色关联的策略列表 示例值：查看
TotalNum	Uint64	角色关联的策略总数 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError.SystemError	内部错误。
InvalidParameter.ParamError	非法入参。

查询策略关联的实体列表

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（ListEntitiesForPolicy）可用于查询策略关联的实体列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-02 21:20:38。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ListEntitiesForPolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	是	否	Uint64	策略 id 示例值： 524497
Page	否	否	Uint64	页码，默认值是 1，从 1 开始 示例值： 1
Rp	否	否	Uint64	每页大小，默认值是 20 示例值： 10
EntityFilter	否	否	String	可取值 'All'、'User'、'Group' 和 'Role'，'All' 表示获取所有实体类型，'User' 表示只获取子账号，'Group' 表示只获取用户组，'Role' 表示只获取角色，默认取 'All' 示例值： All

3. 输出参数

参数名称	类型	描述
TotalNum	Uint64	实体总数 示例值： 1
List	Array of AttachEntityOfPolicy	实体列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.PolicyIdError	输入参数PolicyId不合法。
InvalidParameter.ParamError	非法入参。
InternalError.SystemError	内部错误。

查询策略列表

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（ListPolicies）可用于查询策略列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-09 17:18:22。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ListPolicies
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Rp	否	否	Uint64	每页数量，默认值是 20，必须大于 0 且小于或等于 200 示例值： 1
Page	否	否	Uint64	页码，默认值是 1，从 1开始，不能大于 200 示例值： 10
Scope	否	否	String	可取值 'All'、'QCS' 和 'Local'，'All' 获取所有策略，'QCS' 只获取预设策略，'Local' 只获取自定义策略，默认取 'All' 示例值： All
Keyword	否	否	String	按策略名匹配 示例值： name
TargetUin	否	否	Uint64	按Uin匹配 示例值： 10093
TargetGroupId	否	否	Uint64	按组Id匹配 示例值： 10093

参数名称	必选	允许NULL	类型	描述
TargetRoleId	否	否	Uint64	按角色Id匹配 示例值： 10093
ServiceType	否	否	String	按产品Id匹配，如cvm 示例值： cvm
FlagUin	否	否	Uint64	按Uin标记关联 示例值： 10093
FlagGroupId	否	否	Uint64	按GroupId标记关联 示例值： 10093
FlagRoleId	否	否	Uint64	按角色Id标记关联 示例值： 10093
Order	否	否	String	策略排序参数 示例值： desc
ProjectVisible	否	否	Uint64	项目可见性 示例值： 1
Client	否	否	String	客户端 示例值： console

3. 输出参数

参数名称	类型	描述
TotalNum	Uint64	策略总数 示例值： 239
List	Array of StrategyInfo	策略数组，数组每个成员包括 policyId、policyName、addTime、type、description、 createMode 字段。其中： policyId：策略 id policyName：策略名 addTime：策略创建时间 type：1 表示自定义策略，2 表示预设策略 description：策略描述 createMode：1 表示按业务权限创建的策略，其他值表示可以查看策略语法和通过策略语法更新策略 Attachments: 关联的用户数 ServiceType: 策略关联的产品 IsAttached: 当需要查询标记实体是否已经关联策略时不为null。0表示未关联策略，1表示已关联策略

参数名称	类型	描述
		示例值：查看
ServiceTypeList	Array of String	服务列表 示例值： ["cvm"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
InvalidParameter.UinError	Uin字段不合法。
InternalError.SystemError	内部错误。
InvalidParameter.ScopeError	Scope字段不合法。
InvalidParameter.KeywordError	Keyword字段不合法。
InvalidParameter.GroupIdError	GroupId字段不合法。
InvalidParameter.ServiceTypeError	ServiceType字段不合法。

修改角色信任策略

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（UpdateAssumeRolePolicy）用于修改角色信任策略的策略文档。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:02:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateAssumeRolePolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RoleId	否	否	String	角色ID，用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： 4611686018427731422
RoleName	否	否	String	角色名称，用于指定角色，入参 RoleId 与 RoleName 二选一 示例值： QCS_RoleName
PolicyDocument	是	否	String	策略文档，示例：{"version":"2.0","statement":[{"action":"name/sts:AssumeRole","effect":"allow","principal":{"service":["cloudaudit.<no value>","cls.<no value>"]}}]}，principal用于指定角色的授权对象。获取该参数可参阅 获取角色详情（https://<no value>/document/product/598/36221）输出参数RoleInfo 示例值： {"version":"2.0","statement":[{"action":"sts:AssumeRole","effect":"allow","principal":{"qcs":["qcs::cam::uin/110000000007:root"]}}]}

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ConditionError	策略文档的condition字段不合法。
InvalidParameter.VersionError	策略文档的Version字段不合法。
InternalError.SystemError	内部错误。
InvalidParameter.AttachmentFull	principal字段的授权对象关联策略数已达到上限。
InvalidParameter.PrincipalError	策略文档的principal字段不合法。
InvalidParameter.RoleNotExist	角色不存在。
InvalidParameter.ParamError	非法入参。

更新策略

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口（UpdatePolicy ）可用于更新策略。
如果已存在策略版本，本接口会直接更新策略的默认版本，不会创建新版本，如果不存在任何策略版本，则直接创建一个默认版本。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:02:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdatePolicy
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
PolicyId	是	否	Uint64	策略ID 示例值： 17698703
PolicyName	否	否	String	策略名 示例值： QCS_PolicyName
Description	否	否	String	策略描述 示例值： Policy_Description
PolicyDocument	否	否	String	策略文档，示例：{"version":"2.0","statement":[{"action":"name/sts:AssumeRole","effect":"allow","principal":{"service":["cloudaudit.<no value>","cls.<no value>"]}}]}，principal用于指定角色的授权对象。获取该参数可参阅 获取角色详情（https://<no value>/document/product/598/36221）输出参数RoleInfo 示例值： {"version":"2.0","statement":[{"effect":"allow","action":"cvm:Describe*","resource":"*"}]}

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.PolicyNameError	PolicyName字段不合法。
InvalidParameter.PrincipalError	策略文档的principal字段不合法。
InvalidParameter.ConditionError	策略文档的condition字段不合法。
InvalidParameter.ParamError	非法入参。
InvalidParameter.PolicyDocumentError	PolicyDocument字段不合法。
InvalidParameter.ActionError	策略文档的Action字段不合法。
ResourceNotFound.PolicyIdNotFound	PolicyId指定的资源不存在。
InvalidParameter.NotSupportProduct	CAM不支持策略文档中所指定的资源类型。
InvalidParameter.PolicyDocumentLengthOverLimit	PolicyDocument字段超过长度限制。
ResourceNotFound.UserNotExist	用户不存在。
InternalError.SystemError	内部错误。
InvalidParameter.StatementError	策略文档的Statement字段不合法。
InvalidParameter.VersionError	策略文档的Version字段不合法。
InvalidParameter.EffectError	策略文档的Effect字段不合法。
InvalidParameter.PolicyIdNotExist	策略ID不存在。
InvalidParameter.PolicyIdError	输入参数PolicyId不合法。
InvalidParameter.ResourceError	策略文档的Resource字段不合法。
InvalidParameter.UserNotExist	用户对象不存在。
ResourceNotFound.GroupNotExist	用户组不存在。
ResourceNotFound.NotFound	资源不存在。

错误码	描述
FailedOperation.PolicyNameInUse	PolicyName字段指定的策略名已存在。
InvalidParameter.AttachmentFull	principal字段的授权对象关联策略数已达到上限。
UnauthorizedOperation	未授权操作
InvalidParameter.DescriptionLengthOverlimit	Description入参长度不能大于300字节。

用户相关接口
获取CAM密码规则

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

本接口{GetPasswordRules}用于获取用户的密码设置规则

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-23 16:09:45。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：GetPasswordRules
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
Rules	PasswordRules	密码规则列表 示例值：查看
UpdateTime	String	更新时间 示例值： 2019-04-29 21:18:28
Modifier	String	更新用户 示例值： 130000000001

参数名称	类型	描述
BlackList	String	黑名单字符串列表json string 示例值： aaa
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

子账户所属用户组列表

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

查询子账户所属用户组列表

默认接口请求频率限制：20次/秒。

接口更新时间：2025-04-23 15:09:13。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：GetSubsGroup
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Uid	是	否	Uint64	接收者用户id 示例值： 1258042
Rp	是	否	Int64	单页数量 示例值： 20
Page	是	否	Int64	分页数 示例值： 1

3. 输出参数

参数名称	类型	描述
TotalNum	String	总体数量 示例值： 1

参数名称	类型	描述
GroupInfo	Array of GroupInfo	用户信息列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError.SystemError	内部错误。

根据SecretId查询Uin

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

根据SecretId查询Uin

默认接口请求频率限制：20次/秒。

接口更新时间：2025-03-17 18:04:03。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：GetUinBySecretId
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
ApiSecretId	是	否	String	密钥ID 示例值： AK****

3. 输出参数

参数名称	类型	描述
Uin	Uint64	用户ID 示例值： 100
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。

更新CAM密码规则

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

更新用户密码设置规则

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:06:02。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdatePasswordRules
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Rules	是	否	PasswordRules	密码设置规则 示例值：查看
BlackList	否	否	String	黑名单字符串列表json string 示例值： aaa

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

身份提供商接口
新增oauth配置

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

新增oauth配置

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-12 19:35:47。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateOauthProvider
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Name	是	否	String	身份提供商（企业）名称。示例值: oauthserver 示例值： name
Desc	否	否	String	备注。示例值: mark 示例值： desc
ClientId	是	否	String	注册应用的id。示例值: c1aa4fbce389206a7061 示例值： c1aa4fbce389206a7061
ClientSecret	是	否	String	注册应用的密钥。示例值: 837c669d84f2fe64b11a8853d521a17970df55ca 示例值：944218ad060c8f2483d4d5bbfa64b6256b78aa79
AuthorizeUri	是	否	String	oauth验证授权信息url。示例值: http://test.com/oauth/authorize 示例值： https://github.com/login/oauth/authorize

参数名称	必选	允许NULL	类型	描述
AccessTokenUri	是	否	String	获取access_token url。示例值: http://test.com/oauth/token 示例值： https://github.com/login/oauth/access_token
GetUserInfoUri	是	否	String	获取用户信息url。示例值: http://test.com/oauth/userinfo 示例值： https://api.github.com/user
UserNameField	是	否	String	登录账号对应字段名称。示例值: username 示例值： user
NickNameField	否	否	String	昵称对应字段名称。示例值: nickname 示例值： nick
PhoneNumField	是	否	String	手机号对应字段名称。示例值: phone 示例值： phone
EmailField	是	否	String	邮箱对应字段名称。示例值: email 示例值： email
IsSyncIdpUser	否	否	Int64	是否同步 idp 用户。传0代表不同步, 传1代表同步。示例值: 0 示例值： 0

3. 输出参数

参数名称	类型	描述
Id	Int64	id 示例值： 1
Name	String	名称 示例值： name
SAMLProviderArn	String	SAMLProviderArn 示例值： ""
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation.IdentityExist	身份认证失败。

获取用户oauth标识

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

获取用户第三方开放平台的access token

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:05:48。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：GetUserAccessToken
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
UserAuthCode	是	否	String	auth code授权码 示例值： ""
OpenAccessToken	否	否	String	第三方access token，复杂授权使用。 示例值： d1e459383977a892fa7b6c549d2f76f8

3. 输出参数

参数名称	类型	描述
AppId	String	app id 示例值： 1255000002
UserOpenId	String	第三方openId 示例值： e5fcfd7cf67d62c85d38b10171641c57

参数名称	类型	描述
UserUnionId	String	第三方unionId 示例值： a64e5abe67a8712c348c547a2760f9ce
UserAccessToken	String	第三方access token 示例值： 905dd67ae2a97e9870364a87d7872da2
ExpiresAt	Int64	过期时间 示例值： 1730433390
UserRefreshToken	String	refresh token 示例值： 905dd67ae2a97e9870364a87d7872da2
Scope	String	授权范围 示例值： login
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InvalidParameter.ParamError	非法入参。
InternalError.SystemError	内部错误。
FailedOperation.AuthCodeError	授权码异常。

刷新用户userAccessToken

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

刷新用户第三方access_token

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:05:48。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：RefreshUserToken
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
UserRefreshToken	是	否	String	用户刷新token 示例值： d1e459383977a892fa7b6c549d2f76f8
UserOpenId	是	否	String	用户openId 示例值： e5fcfd7cf67d62c85d38b10171641c57

3. 输出参数

参数名称	类型	描述
UserAccessToken	String	第三方access_token 示例值： d1e459383977a892fa7b6c549d2f76f8
ExpiresAt	Int64	过期时间 示例值： 1730433390

参数名称	类型	描述
AppId	String	appId 示例值： 1255000002
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation.RefreshTokenError	刷新用户token异常。
InvalidParameter.ParamError	非法入参。
InternalError.SystemError	内部错误。

更新Oauth配置信息

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

更新Oauth配置信息

默认接口请求频率限制：20次/秒。

接口更新时间：2022-11-16 17:05:50。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpdateOauthProvider
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Desc	否	否	String	备注 示例值： desc
Name	是	否	String	身份提供商（企业）名称 示例值： name
Id	是	否	Int64	id 示例值： 1
OwnerUin	是	否	Int64	OwnerUin 示例值： 110000000001
ClientId	是	否	String	注册应用的id 示例值： c1aa4fbce389206a7061
ClientSecret	是	否	String	注册应用的密钥 示例值： 944218ad060c8f2483d4d5bbfa64b6256b78aa79

参数名称	必选	允许NULL	类型	描述
AuthorizeUri	是	否	String	oauth验证授权信息url 示例值： https://github.com/login/oauth/authorize
AccessTokenUri	是	否	String	获取access_token url 示例值： https://github.com/login/oauth/access_token
GetUserInfoUri	是	否	String	获取用户信息url 示例值： https://api.github.com/user
UserNameField	是	否	String	登录账号对应字段名称 示例值： user
NickNameField	否	否	String	昵称对应字段名称 示例值： nick
PhoneNumField	是	否	String	手机号对应字段名称 示例值： phone
EmailField	是	否	String	邮箱对应字段名称 示例值： email
IsSyncIdpUser	是	否	Int64	是否同步 idp 用户数据 示例值： 0

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

验证用户userAccessToken

1. 接口描述

接口请求域名： cam.api3.finance.cloud.tencent.com。

验证用户第三方开放平台access_token

默认接口请求频率限制：20次/秒。

接口更新时间：2022-08-11 19:05:48。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：VerifyUserAccessToken
Version	是	否	String	公共参数，本接口取值：2019-01-16
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
UserAccessToken	是	否	String	access token 示例值： d1e459383977a892fa7b6c549d2f76f8
UserOpenId	是	否	String	open id 示例值： e5fcfd7cf67d62c85d38b10171641c57

3. 输出参数

参数名称	类型	描述
UserOpenId	String	第三方平台openId 示例值： e5fcfd7cf67d62c85d38b10171641c57
UserUnionId	String	第三方平台unionId 示例值： d1e459383977a892fa7b6c549d2f76f8
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
FailedOperation.UserrAccessTokenError	用户接入token异常。
InvalidParameter.ParamError	非法入参。
InternalError.SystemError	内部错误。

数据结构

AttachedUserPolicy

用户关联的策略详情

被如下接口引用：ListAttachedUserAllPolicies

名称	必选	允许NULL	类型	描述
PolicyId	否	否	Uint64	策略ID 示例值： 1000
PolicyName	否	否	String	策略名 示例值： policygen-20141112201913
Description	否	否	String	策略描述 示例值： adesc
AddTime	否	否	String	创建时间 示例值： 2014-08-03 12:00:00
StrategyType	否	否	Uint64	策略类型(1表示自定义策略，2表示预设策略) 示例值： 1
CreateMode	否	否	Uint64	创建模式(1表示按产品或项目权限创建的策略，其他表示策略语法创建的策略) 示例值： 1
Groups	否	是	Array of AttachedUserPolicyGroupInfo	随组关联信息 示例值：查看

ServiceItem

服务

被如下接口引用：GetServiceList

名称	必选	允许NULL	类型	描述
AddTime	否	否	Datetime	创建时间

名称	必选	允许NULL	类型	描述
				示例值： 2014-08-03 12:00:00
ArnDocument	否	否	String	ArnDocument 示例值： https://www.example.com/document/product/378/8222965
ColConf	否	是	String	ColConf 示例值： ColConf
DefAddr	否	是	String	DefAddr 示例值： DefAddr
DefaultStrategyList	否	否	String	默认策略 示例值： DefaultStrategyList
IsAllowDefProj	否	否	String	IsAllowDefProj 示例值： 1
IsDisProject	否	否	String	IsDisProject 示例值： 1
IsDisZone	否	否	String	IsDisZone 示例值： 1
IsSeen	否	否	String	是否可见 示例值： 1
Online	否	否	String	Online 示例值： Online
QueryAddr	否	否	String	QueryAddr 示例值： cvm
QueryInterface	否	否	String	QueryInterface 示例值： cvm
ServiceEnName	否	否	String	服务英文名 示例值： cvm
ServiceName	否	否	String	服务名 示例值： cvm
ServiceType	否	否	String	服务类型 示例值： cvm
SynInterface	否	否	String	SynInterface 示例值： cvm

名称	必选	允许NULL	类型	描述
UpdateTime	否	否	Datetime	变更时间 示例值： 2014-08-03 12:00:00
Weight	否	否	String	Weight 示例值： 1
WhiteKey	否	否	String	WhiteKey 示例值： white1
Writter	否	否	String	创建人 示例值： admin
ResourceTypeList	否	否	Array of ResourceTypeItem	资源类型数组 示例值：查看
Type	否	否	String	类型 示例值： cvm

UserList

子账号列表

被如下接口引用：ListUsersForPolicy

名称	必选	允许NULL	类型	描述
Name	是	否	String	子账号名称 示例值： admin
SubAccountUin	是	否	String	子账号uin 示例值： 1000

OwnerAccountAttribute

主账户属性

被如下接口引用：UpdateOwnerAccount

名称	必选	允许NULL	类型	描述
Remark	否	否	String	属性 示例值： remark

PasswordRules

密码规则

被如下接口引用：GetPasswordRules、UpdatePasswordRules

名称	必选	允许NULL	类型	描述
MinimumLength	是	否	Int64	最小密码长度 示例值： 10
MustContain	是	否	String	最少包含 示例值： Aa!
ForcePasswordChange	是	否	Int64	密码有效期 示例值： 0
ReusePasswordLimit	是	否	Int64	密码重复次数 示例值： 2
RetryPasswordLimit	否	否	Int64	登陆最大密码失败次数 示例值： 2
OnlyAdminCanResetPassword	否	否	Int64	是否只有admin可以重置密码 示例值： 0
MustNotContainUsername	否	否	Int64	必须不包含用户名 示例值： 0

SubAccountFilter

带过滤条件的子帐号信息

被如下接口引用：GetGroupList、GetGroupsSubAccount、GetSubsGroup、ListGroups、ListGroupsForConsole、ListMaskedSubAccounts、ListSubAccounts

名称	必选	允许NULL	类型	描述
Uid	是	是	Uint64	子用户Uid 示例值： 1258042
Uin	是	是	Uint64	用户Uin 示例值： 130000000001

名称	必选	允许NULL	类型	描述
Name	是	是	String	用户Name 示例值： username
Remark	是	是	String	备注 示例值： remark
CanLogin	是	是	Uint64	是都允许登录 示例值： 1
PhoneNum	是	是	String	电话号码 示例值： 11111111111
CountryCode	是	是	String	区号 示例值： 86
PhoneFlag	是	是	Int64	电话号码是否验证 示例值： 1
Email	是	是	String	邮箱 示例值： mail@mail.com
EmailFlag	是	是	Int64	邮箱是否验证 示例值： 1
UserType	是	是	Int64	用户类型 示例值： 0
CreateTime	是	是	String	创建时间 示例值： 2019-04-29 21:18:28
IsReceiverOwner	是	是	Int64	是否消息接收人 示例值： 1
SystemType	是	是	String	类型 示例值： subaccount
NeedResetPassword	是	是	Int64	是否需要重置密码 示例值： 0
ConsoleLogin	是	是	Int64	是否允许控制台登录 示例值： 1
WxzsStatus	是	是	Int64	微信公众号关注状态 示例值： 0

名称	必选	允许NULL	类型	描述
PermType	是	是	Array of String	权限类型 示例值： ["0"]
NickName	是	是	String	昵称 示例值： nick
QywxUserId	否	否	String	企业微信用户id 示例值： qywxuserid
UserAttributeAndValues	否	是	Array of AccountAttributeAndValue	扩展属性 示例值：查看
Status	否	否	Int64	状态 示例值： 0
LoginStatus	否	否	Int64	登陆状态 示例值： 0
VerifyPhone	否	否	String	VerifyPhone 示例值： 11111111111
VerifyEmail	否	否	String	VerifyEmail 示例值： mail@mail.com
VerifyCountryCode	否	否	String	VerifyCountryCode 示例值： 86

SubAccountInfo

子账户用户信息

被如下接口引用：UpdateSubAccount

名称	必选	允许NULL	类型	描述
CanLogin	否	否	String	能否登陆，0-否，1-可 示例值： 1
ConsoleLogin	否	否	String	是否是控制台登陆，1-是 示例值： 1
CountryCode	否	否	String	国家编码 示例值： 86

名称	必选	允许NULL	类型	描述
Name	否	否	String	用户名 示例值： 名称
NeedResetPassword	否	否	String	是否需要重置密码，1-是 示例值： 0
PhoneNum	否	否	String	手机号 示例值： 11111111111
Remark	否	否	String	备注 示例值： 备注
SystemType	否	否	String	账户类型 示例值： subaccount
Uid	否	否	String	接收者用户ID 示例值： 1280504
Uin	否	否	String	账户唯一id 示例值： 110000000001
Password	否	否	String	密码 示例值： password
WxzsStatus	否	否	Int64	微信消息状态 示例值： 0
UserType	否	否	Int64	用户类型 示例值： 0
Email	否	否	String	联系邮箱 示例值： mail@mail.com
Account	否	否	String	用户名 示例值： username
Lang	否	否	String	语言 示例值： en-US
NickName	否	否	String	昵称 示例值： 昵称

GroupData

用户组相关信息

被如下接口引用：GetAllSubUser

名称	必选	允许NULL	类型	描述
GroupId	否	否	Int64	用户组id 示例值： 1000
GroupName	是	否	String	用户组名称 示例值： group1
GroupNum	是	否	Int64	用户组成员数量 示例值： 100
Channel	是	否	Int64	创建渠道 示例值： 0
GroupMem	否	否	Array of Uint64	组成员uid 示例值： [1280504,1280505]

ApiKey

API密钥数据列表

被如下接口引用：CreateApiKey、CreateCollApiKey、QueryApiKey、QueryCollApiKey、QueryKeyBySecretId

名称	必选	允许NULL	类型	描述
SecretId	否	否	String	密钥ID 示例值： AKID***wdew
CreateTime	否	否	Uint64	创建时间(时间戳) 示例值： 1615990212
Status	否	否	Uint64	状态(2:有效, 3:禁用) 示例值： 2
SecretKey	否	否	String	密钥Key 示例值： ACCF***wdew
Source	否	否	Uint64	来源 示例值： 0
Remark	否	否	String	备注 示例值： remark

GroupMeta

用户组元信息

被如下接口引用：GetUserGroupList、ListAllUserGroup

名称	必选	允许NULL	类型	描述
GroupId	否	是	Int64	用户组id 示例值： 100
GroupName	否	是	String	用户组名称 示例值： group1

OwnerInfo

主账号信息

被如下接口引用：ListMaskedSubAccounts、ListSubAccounts

名称	必选	允许NULL	类型	描述
Uin	是	是	Uint64	主帐号Uin 示例值： 130000000001
UserName	是	是	String	用户名 示例值： username
CheckStatus	是	否	Uint64	校验状态 示例值： 0

AccountDetail

账号详情

被如下接口引用：AddSubAccount、ListGroups

名称	必选	允许NULL	类型	描述
ActionFlag	否	否	ActionLoginFlag	敏感操作标识 示例值：查看
ConsoleLogin	否	否	String	是否允许控制台登录, 传0不可登陆控制台, 传1可以登陆控制台。示例值: 1

名称	必选	允许NULL	类型	描述
				示例值： 1
LoginFlag	否	否	ActionLoginFlag	登录保护 示例值：查看
NeedResetPassword	否	否	String	是否需要重置密码, 传0不需要重置密码, 传1需要重置密码。示例值: 0 示例值： 0
Password	否	否	String	用户密码。示例值: password 示例值： password
UseApi	否	否	String	使用Api, 传0不使用Api, 传1使用Api。 示例值: 1 示例值： 1
TokenType	否	否	Int64	分配设备类型,传0不分配设备,传2分配设备。示例值: 0 示例值： 0

GroupUidUinInfo

用户组和用户信息

被如下接口引用：DeleteSubAccount

名称	必选	允许NULL	类型	描述
Uid	是	否	Uint64	子用户Uid 示例值： 1258042
Uin	是	否	Uint64	子用户Uin 示例值： 130000000001
GroupId	是	否	Int64	用户组ID 如果没有任何组传递-1,传入指定组id表示将用户从组删除 示例值： 15094

ApiKeyDetail

持久密钥详情

被如下接口引用：GetApiKey

名称	必选	允许NULL	类型	描述
SecretId	否	否	String	密钥ID 示例值： AK**********
SecretKey	否	否	String	密钥Key 示例值： TR**********
CreateTime	否	否	Uint64	创建时间(时间戳) 示例值： 2014-08-03 12:00:00
Status	否	否	Uint64	状态(2:有效, 3:禁用) 示例值： 1
Source	否	否	Uint64	来源，默认0 示例值： 1
Remark	否	是	String	描述 示例值： aremark

AttachEntityOfPolicy

策略关联的实体信息

被如下接口引用：ListEntitiesForPolicy

名称	必选	允许NULL	类型	描述
Id	是	否	String	实体ID 示例值： 1000001
Name	是	是	String	实体名称 示例值： policygen-20141112201913
Uin	是	是	Uint64	实体Uin 示例值： 3449203261
RelatedType	是	否	Uint64	关联类型。1 用户关联 ； 2 用户组关联 示例值： 1

AttachedStrategyInfo

策略信息

被如下接口引用：DescribeAttachedEntityPolicies

名称	必选	允许NULL	类型	描述
PolicyId	否	否	Uint64	策略ID。 示例值： 1000
PolicyName	否	否	String	策略名称。 示例值： policygen-20141112201913
AddTime	否	是	Datetime	策略创建时间。 示例值： 2014-08-03 12:00:00
CreateMode	否	是	Uint64	创建来源，1 通过控制台创建, 2 通过策略语法创建。 示例值： 1
Description	否	是	String	策略描述。 示例值： adesc

ServicePermItem

接口

被如下接口引用：GetServicePermList

名称	必选	允许NULL	类型	描述
AddTime	否	否	Datetime	创建时间 示例值： 2014-08-03 12:00:00
ApiAddr	否	否	String	ApiAddr 示例值： ApiAddr
ApiZhName	否	否	String	中文描述 示例值： ADMIN
AuthFunction	否	否	String	鉴权接口 示例值： AuthFunction
CWildcardName	否	否	String	CWildcardName 示例值： CWildcardName
InterfaceEnName	否	否	String	接口名 示例值： CVM
InterfaceLevel	否	否	String	鉴权粒度，0:接口级别、1:资源级别 示例值： 1

名称	必选	允许NULL	类型	描述
IsAuthBusiness	否	否	String	鉴权方式，0:由云API转发鉴权、1:业务自行调用鉴权接口 示例值： 1
IsNeedObject	否	否	String	IsNeedObject 示例值： 1
IsSeen	否	否	Uint64	IsSeen 示例值： 1
IsSeenAtGenerator	否	否	String	策略生成器是否可见 示例值： 1
IsSpResource	否	否	String	IsSpResource 示例值： 1
IsUserSet	否	否	String	IsUserSet 示例值： 1
PermId	否	否	String	Id 示例值： 1000
ReadWriteDetail	否	否	String	接口类别 示例值： 接口类别：0.读取，1.写入，2.标记，3.列表
ResourceType	否	是	String	资源类别 示例值： cvm
UpdateTime	否	否	String	更新时间 示例值： 2014-08-03 12:00:00
Weight	否	否	String	Weight 示例值： 1
Writter	否	否	String	操作者 示例值： admin
ServiceName	否	否	String	服务名 示例值： cvm
ProductShortCode	否	否	String	ProductShortCode 示例值： p_cvm
ProductShortName	否	否	String	ProductShortName 示例值： p_cvm

名称	必选	允许NULL	类型	描述
ServiceType	否	否	String	服务类型 示例值： cvm
Interface	否	否	String	接口名 示例值： CVM
InterfaceName	否	否	String	接口名 示例值： CVM

ListOpenPlatform

第三方平台详细信息

被如下接口引用：ListOpenPlatforms

名称	必选	允许NULL	类型	描述
OpenId	是	否	Int64	openid 示例值： 1
AppId	是	否	String	app id 示例值： 1255000002
OpenName	是	否	String	app name 示例值： ""
OpenLogo	是	否	String	open logo 示例值： ""
OpenHome	是	否	String	第三方平台主页 示例值： ""
OpenType	是	否	Int64	授权类型 示例值： 0
Uin	是	否	Uint64	申请账号 示例值： 110000000001
Status	是	否	Int64	状态 示例值： 0
Domain	是	否	String	第三方平台域名 示例值： ""

名称	必选	允许NULL	类型	描述
State	是	否	Int64	冻结状态，0-非冻结，1-冻结 示例值： 0
Modifier	是	否	String	修改人 示例值： 110000000001
ModifyTime	是	否	String	更新时间 示例值： 2019-04-29 21:18:28
CreateTime	是	否	String	创建时间 示例值： 2019-04-29 21:18:28
Memo	是	否	String	备注 示例值： ""

UserInfo

用户信息

被如下接口引用：AddSubAccount、ListGroups

名称	必选	允许NULL	类型	描述
CanLogin	否	否	String	子账号类型，传0不可登陆控制台，传1可以登陆控制台。 示例值： 1
CountryCode	否	否	String	区号。 示例值： 86
Detail	否	否	AccountDetail	详情 示例值：查看
Name	否	否	String	名称。 示例值： name
PhoneNum	否	否	String	电话号码。 示例值： 11111111111
SystemType	否	否	String	账号类型。 示例值： Subaccount
Email	否	否	String	安全邮箱。 示例值： mail@mail.com

名称	必选	允许NULL	类型	描述
NickName	否	否	String	昵称。 示例值： nickname
Remark	否	否	String	备注。 示例值： remark
WxzsStatus	否	否	Int64	微信登陆状态。 示例值： 0
ContactMail	否	否	String	联系邮箱。 示例值： mail@mail.com
IsReceiverOwner	否	否	Int64	是否是主账号。传1代表主账号, 传0代表子账号。 示例值： 1
IdentifyType	否	否	Int64	身份类型。 示例值： 0

AttachPolicyInfo

关联策略信息

被如下接口引用：ListAttachedGroupPolicies

名称	必选	允许NULL	类型	描述
PolicyId	是	否	Uint64	策略id 示例值： 1000
PolicyName	是	是	String	策略名称 示例值： policygen-20141112201913
AddTime	是	是	Datetime	创建时间 示例值： 2014-08-03 12:00:00
CreateMode	是	是	Uint64	创建来源，1 通过控制台创建, 2 通过策略语法创建。 示例值： 1

GroupMember

用户组成员

被如下接口引用：AddUserToGroup、RemoveUserFromGroup、UpdateGroupMember

名称	必选	允许NULL	类型	描述
Uid	是	否	String	用户id 示例值： 100
GroupId	是	否	String	组id 示例值： 100

StrategyInfo

策略信息

被如下接口引用：ListPolicies

名称	必选	允许NULL	类型	描述
PolicyId	是	否	Uint64	策略ID。 示例值： 1
PolicyName	是	否	String	策略名称。 示例值： AdministratorAccess
AddTime	是	是	Datetime	策略创建时间。 示例值： 2016-06-02 19:40:09
Type	是	否	Uint64	策略类型。1 表示自定义策略，2 表示预设策略。 示例值： 1
Description	是	是	String	策略描述。 示例值： 该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资产。
CreateMode	是	否	Uint64	创建来源，1 通过控制台创建, 2 通过策略语法创建。 示例值： 1
Attachments	否	否	Uint64	关联的用户数 示例值： 1
ServiceType	是	是	String	策略关联的产品 示例值： cam
IsAttached	否	是	Uint64	当需要查询标记实体是否已经关联策略时不为null。0表示未关联策略，1表示已关联策略 示例值： 1

名称	必选	允许NULL	类型	描述
Deactived	否	是	Uint64	是否已下线，传1代表已下线，传0代表未下线 示例值： 0
DeactivedDetail	否	是	Array of String	已下线产品列表 示例值： ["deacproduct"]
IsCheck	是	是	Uint64	是否进行安全性校验，传1代表进行安全校验，传0代表不校验 示例值： 1
PolicyDocument	否	否	String	策略语法 示例值： {\"version\":\"2.0\",\"statement\":[{\"effect\":\"allow\",\"action\":[\"cvm:ModifyDiskAttributes\"],\"resource\":[\"*\"],\"condition\":{\"ip_equal\":{\"qcs:ip\":[\"1.1.1.1\"]}}},{\"effect\":\"allow\",\"action\":[\"cos:PutObject\"],\"resource\":[\"qcs::cos::uid/1255000018:rules-package-ftp-1255000018/waf_rules.zip\"],\"condition\":{\"ip_equal\":{\"qcs:ip\":[\"1.1.1.1\"]}}}]}
UpdateTime	否	否	String	修改时间 示例值： 2016-06-02 19:40:09

AttributeInfo

属性

被如下接口引用：AddAttributeValues

名称	必选	允许NULL	类型	描述
AttributeName	否	是	String	属性名称 示例值： ""
Attribute	否	是	String	属性 示例值： ""
AttributeValue	否	是	String	属性值 示例值： ""

ResourceTypeItem

资源类型

被如下接口引用：GetServiceList

名称	必选	允许NULL	类型	描述
ResourceEnName	否	否	String	英文名 示例值： ""
ResourceName	否	否	String	中文名 示例值： ""
ResourceType	否	否	String	资源类型 示例值： ""
ServiceType	否	否	String	服务类型 示例值： ""

UserLists

GetUserListByUinList

被如下接口引用：GetUserListByUinList

名称	必选	允许NULL	类型	描述
CountryCode	否	否	String	CountryCode 示例值： 86
IsAuthed	否	否	Int64	IsAuthed 示例值： 0
UserCamUid	否	否	Int64	UserCamUid 示例值： 1280504
UserCellphone	否	否	String	UserCellphone 示例值： 11111111111
UserEmail	否	否	String	UserEmail 示例值： mail@mail.com
UserId	否	否	String	UserId 示例值： 1280504
UserUin	否	否	Uint64	UserUin 示例值： 110000000001

名称	必选	允许NULL	类型	描述
UserName	否	否	String	UserName 示例值： username
UserIsLocked	否	否	Int64	UserIsLocked 示例值： 1

FilterItem

过滤条件数据结构

被如下接口引用：ListMaskedSubAccounts、ListSubAccounts

名称	必选	允许NULL	类型	描述
Operator	是	否	String	操作符 示例值： ""
Attr	是	否	String	属性 示例值： ""
Value	是	否	String	匹配值 示例值： ""

RoleInfo

角色详细信息

被如下接口引用：DescribeRoleList、GetRole

名称	必选	允许NULL	类型	描述
RoleId	是	否	String	角色ID 示例值： 12
RoleName	是	否	String	角色名称 示例值： QCS
PolicyDocument	是	否	String	角色的策略文档 示例值： {\"version\":\"2.0\",\"statement\":[{\"effect\":\"allow\",\"action\":[\"cvm:ModifyDiskAttributes\"],\"resource\":[\"*\"],\"condition\":{\"ip_equal\":{\"qcs:ip\":[\"1.1.1.1\"]}}},{\"effect\":\"allow\",\"action\":

名称	必选	允许NULL	类型	描述
				[\"cos:PutObject\"],\"resource\":[\"qcs::cos::uid/1255000018:rules-package-ftp-1255000018/waf_rules.zip\"],\"condition\":{\"ip_equal\":{\"qcs:ip\":[\"1.1.1.1\"]}}}]}
Description	是	否	String	角色描述 示例值： Description
AddTime	是	否	String	角色的创建时间 示例值： 2020-01-01 01:01:01
UpdateTime	是	否	String	角色的最近一次时间 示例值： 2020-01-01 01:01:01
DeletionTaskId	否	是	String	兼容公有云字段，无含义 示例值： 1
ConsoleLogin	是	否	Uint64	角色是否允许登录，传1代表允许登录，传0代表不允许 示例值： 1
RoleType	否	是	String	角色类型，取user、system或service_linked 示例值： user
SessionDuration	否	是	Uint64	有效时间 示例值： 7200

RolePolicyList

角色策略列表

被如下接口引用：GetServiceRoleInfo

名称	必选	允许NULL	类型	描述
IsHidden	否	否	Uint64	状态 示例值： 1
PolicyId	否	否	String	策略Id 示例值： 100
PolicyName	否	否	String	策略名 示例值： policygen-20141112201913

AttachedPolicyOfRole

角色关联的策略信息

被如下接口引用：ListAttachedRolePolicies

名称	必选	允许NULL	类型	描述
PolicyId	是	否	Uint64	策略ID 示例值： 1000
PolicyName	是	否	String	策略名称 示例值： policygen-20141112201913
AddTime	是	否	String	绑定时间 示例值： 2014-08-03 12:00:00
PolicyType	是	是	String	策略类型，User表示自定义策略，QCS表示预设策略 示例值： 按策略类型过滤，User表示仅查询自定义策略，QCS表示仅查询预设策略
CreateMode	是	否	Uint64	策略创建方式，1表示按产品功能或项目权限创建，其他表示按策略语法创建 示例值： 1

Filter

过滤条件组合

被如下接口引用：ListMaskedSubAccounts、ListSubAccounts

名称	必选	允许NULL	类型	描述
Keywords	否	否	Array of FilterItem	过滤条件组合 示例值：查看
Operator	是	否	String	操作符 示例值： ""

GroupInfoWithRemark

GroupInfoWithRemark

被如下接口引用：ListUsersForGroup

名称	必选	允许NULL	类型	描述
GroupId	否	否	Int64	GroupId 示例值： 100
GroupName	否	否	String	GroupName 示例值： name
Remark	否	否	String	Remark 示例值： remark

AddSubAccountDetail

新增用户详情

被如下接口引用：AddSubAccount

名称	必选	允许NULL	类型	描述
Name	否	否	String	用户名 示例值： name
Token	否	否	String	token 示例值： ""
Password	否	否	String	密码 示例值： password
SecretId	否	否	String	secretid 示例值： ""
SecretKey	否	否	String	secretKey 示例值： ""
NickName	否	否	String	昵称 示例值： nickname
Uin	否	否	Uint64	uin 示例值： 110000000001
Nickname	否	否	String	Nickname 示例值： nickname

AttachedStrategyInfoPack

策略信息包

被如下接口引用：DescribeAttachedEntityPolicies

名称	必选	允许NULL	类型	描述
List	否	否	Array of AttachedStrategyInfo	策略数组，数组每个成员包括 policyId、policyName、addTime、type、description、 createMode 字段。其中： 示例值：查看
TotalNum	否	否	Uint64	策略数 示例值： 100
Id	否	否	String	入参Type=1时表示uin，2时表示groupId 示例值： 100

ExtAttr

用户属性集合

被如下接口引用：DescribeSubReceiver

名称	必选	允许NULL	类型	描述
NeedResetToken	是	否	Int64	需要重置mfa的token 示例值： 0
NeedResetStoken	是	否	Int64	需要重置mfa的stoken 示例值： 0

UserData

用户信息数据

被如下接口引用：GetAllSubUser

名称	必选	允许NULL	类型	描述
Uid	是	否	Uint64	子用户id 示例值： 1258042
Uin	是	否	Uint64	账号唯一序列号 示例值： 110000000001

名称	必选	允许NULL	类型	描述
Name	是	否	String	用户名称 示例值： name
PhoneNum	是	否	String	电话号码 示例值： 11111111111
CountryCode	是	否	String	区号 示例值： 86
PhoneFlag	是	否	Int64	电话认证标志 示例值： 1
Email	是	否	String	邮箱地址 示例值： mail@mail.com
EmailFlag	是	否	Int64	邮箱是否认证 示例值： 1
UserType	是	否	Int64	用户类型 示例值： 0
CreateTime	是	否	String	创建时间 示例值： 2019-04-29 21:18:28
WechatFlag	是	否	Int64	微信标识 示例值： 0
SystemType	是	否	String	账号系统类型 示例值： Subaccount
IsReceiverOwner	是	否	Int64	是否为主账号 示例值： 1
PermType	否	否	Array of String	PermType 示例值： ["0"]

DescribeGroupsInfo

DescribeGroupsInfo

被如下接口引用：DescribeGroups

名称	必选	允许NULL	类型	描述
Channel	否	否	Int64	Channel

名称	必选	允许NULL	类型	描述
				示例值： 3
CreateTime	否	否	String	CreateTime 示例值： 2025-02-21 11:30:44
GroupId	否	否	Int64	GroupId 示例值： 100
GroupName	否	否	String	GroupName 示例值： name
GroupNum	否	否	Int64	GroupNum 示例值： 3
GroupType	否	否	Int64	GroupType 示例值： 0
Remark	否	否	String	Remark 示例值： Remark
UserInfo	否	否	Array of ListGroupUserInfo	UserInfo 示例值：查看

ServiceApiListInfo

服务的API信息

被如下接口引用：GetServiceApiList

名称	必选	允许NULL	类型	描述
Name	是	否	String	API名称 示例值： CreateInstance
IsNeedObject	是	是	String	是否需要关联对象 示例值： ["1"]
Desc	是	是	String	描述 示例值： 创建实例
ReadWriteDetail	是	是	Uint64	接口类别：0.读取，1.写入，2.标记，3.列表 示例值： 1
InterfaceLevel	是	是	Uint64	授权粒度：0.接口级，1.资源级 示例值： 1

名称	必选	允许NULL	类型	描述
ResourceExample	是	是	String	资源六段式范例 示例值： [qcs::cvm:region:uin/110000001207:volume/*]

GroupInfo

用户组信息

被如下接口引用：GetGroupList、GetGroupsSubAccount、GetSubsGroup、ListGroups、ListGroupsForConsole、ListMaskedSubAccounts、ListSubAccounts

名称	必选	允许NULL	类型	描述
GroupId	否	否	Uint64	组id 示例值： 15094
GroupName	否	否	String	组名称 示例值： groupname
Channel	否	是	Int64	息接收渠道 0:无 1: 短信 2：邮件 3：短信+邮件 示例值： 0
Remark	否	是	String	备注 示例值： remark
CreateTime	否	是	String	创建时间 示例值： 2019-04-29 21:18:28
UserInfo	否	是	Array of SubAccountFilter	用户组成员信息 示例值：查看
GroupType	否	是	Int64	用户组类型，0-自定义，1-预设 示例值： 0
GroupNum	否	否	Int64	组成员数 示例值： 2

GroupUserInfo

用户组下用户信息

被如下接口引用：GetGroupsSubAccount

名称	必选	允许NULL	类型	描述
Uid	是	是	Uint64	接收者用户id 示例值： 1258042
Uin	是	是	Uint64	账户唯一id 示例值： 130000000001
Name	是	是	String	用户名 示例值： username
PhoneNum	是	是	String	手机号 示例值： 11111111111
CountryCode	是	是	String	国家编码 示例值： 86
PhoneFlag	是	是	String	手机号标识 示例值： 1
Email	是	是	String	邮箱 示例值： mail@mail.com
EmailFlag	是	是	String	邮箱标识 示例值： 1
UserType	是	是	Int64	用户类型 示例值： 0
CreateTime	是	是	String	创建时间 示例值： 2019-04-29 21:18:28
IsReceiverOwner	是	是	String	是否是主账户 示例值： 1
SystemType	是	是	String	账户类型 示例值： subaccount
NickName	是	是	String	昵称 示例值： nick

Receiver

消息接收人信息

被如下接口引用：DescribeSubAccountContacts

名称	必选	允许NULL	类型	描述
Uid	是	否	Uint64	id 示例值： 1258042
Name	是	否	String	名字 示例值： username
Remark	是	否	String	备注 示例值： remark
PhoneNumber	是	否	String	手机号码 示例值： 11111111111
PhoneFlag	是	否	Int64	手机号码是否验证 示例值： 1
Email	是	否	String	邮箱 示例值： mail@mail.com
EmailFlag	是	否	Int64	邮箱是否验证 示例值： 1
IsReceiverOwner	是	否	Int64	是否主联系人 示例值： 1
WechatFlag	否	否	Int64	是否允许微信接收通知 示例值： 0
Uin	是	否	Uint64	账号uin 示例值： 130000000001

ListGroupUserInfo

ListGroupUserInfo

被如下接口引用：DescribeGroups、ListUsersForGroup

名称	必选	允许NULL	类型	描述
CountryCode	否	否	String	CountryCode 示例值： 86
CreateTime	否	否	String	CreateTime 示例值： 2025-01-17 14:21:07

名称	必选	允许NULL	类型	描述
Email	否	否	String	Email 示例值： mail@mail.com
EmailFlag	否	是	Int64	EmailFlag 示例值： 0
IsReceiverOwner	否	否	Int64	IsReceiverOwner 示例值： 0
JoinTime	否	否	String	JoinTime 示例值： 2025-01-17 14:21:07
Name	否	否	String	Name 示例值： Name
NickName	否	否	String	NickName 示例值： NickName
PhoneFlag	否	否	Int64	PhoneFlag 示例值： 0
PhoneNum	否	否	String	PhoneNum 示例值： 11111111111
SystemType	否	否	Int64	SystemType 示例值： 0
Uid	否	否	Uint64	Uid 示例值： 1258683
Uin	否	否	Uint64	Uin 示例值： 130000000640
UserType	否	否	Int64	UserType 示例值： 3
QywxUserId	否	否	String	QywxUserId 示例值： ""

ActionLoginFlag

登录操作敏感标识

被如下接口引用：AddSubAccount、ListGroups

名称	必选	允许NULL	类型	描述
Phone	否	否	String	电话, 传0不开启敏感操作保护, 传1开启敏感操作保护。示例值: 0 示例值： 0
Stoken	否	否	String	软Token, 传0不开启敏感操作保护, 传1开启敏感操作保护。示例值: 0 示例值： 0
Token	否	否	String	硬Token, 传0不开启敏感操作保护, 传1开启敏感操作保护。示例值: 0 示例值： 0
Ukey	否	否	String	ukey, 传0不开启敏感操作保护, 传1开启敏感操作保护。示例值: 0 示例值： 0

ServiceApiInfo

服务及其API信息

被如下接口引用：GetServiceApiList

名称	必选	允许NULL	类型	描述
Name	是	否	String	服务名称 示例值： 用户与权限
ServiceType	是	否	String	服务ID 示例值： cam
ArnDocument	是	是	String	服务介绍文档链接 示例值： https://www.example.com/document/product/378/8965
ApiList	否	是	Array of ServiceApiListInfo	API信息列表 示例值：查看
ConditionKeyList	否	是	Array of String	条件规则列表 示例值： ["qcs:ip"]

StrategyInfoForAction

策略详情

被如下接口引用：ListPoliciesByAction

名称	必选	允许NULL	类型	描述
PolicyId	否	否	Uint64	策略ID。 示例值： 1
PolicyName	否	否	String	策略名称。 示例值： AdministratorAccess
AddTime	否	否	Datetime	策略创建时间。 示例值： 2016-06-02 19:40:09
Type	否	否	Uint64	策略类型。1 表示自定义策略，2 表示预设策略。 示例值： 1
Description	否	否	String	策略描述。 示例值： 该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资产。
CreateMode	否	否	Uint64	创建来源，1 通过控制台创建, 2 通过策略语法创建。 示例值： 1
Attachments	否	是	Uint64	关联的用户数 示例值： 1
ServiceType	否	否	String	策略关联的产品 示例值： cam
IsAttached	否	是	Uint64	当需要查询标记实体是否已经关联策略时不为null。0表示未关联策略，1表示已关联策略 示例值： 1
Deactived	否	是	Uint64	是否已下线，传1代表已下线，传0代表未下线 示例值： 0
DeactivedDetail	否	是	Array of String	已下线产品列表 示例值： ["cvm"]
IsCheck	否	是	String	是否进行安全性校验，传1代表进行安全校验，传0代表不校验 示例值： 1
PolicyDocument	否	否	String	策略语法 示例值： {"version":"2.0","statement":[{"action":["cam:*","account:*"],"resource":["*"],"effect":"allow"}]}
UpdateTime	否	否	String	修改时间 示例值： 2016-06-02 19:40:09

UserGroup

用户及用户组信息

被如下接口引用：GetUserGroupList、ListAllUserGroup

名称	必选	允许NULL	类型	描述
Uid	是	是	Uint64	接收者用户id 示例值： 1258042
Uin	是	是	Uint64	账户唯一id 示例值： 110000000001
Name	是	是	String	用户名 示例值： name
IsReceiverOwner	是	是	Int64	是否是主账户 示例值： 1
Group	是	是	Array of GroupMeta	用户组信息 示例值：查看

AttachedUserPolicyGroupInfo

用户关联策略(随组管理)信息

被如下接口引用：ListAttachedUserAllPolicies

名称	必选	允许NULL	类型	描述
GroupId	否	否	Uint64	分组ID 示例值： 10012
GroupName	否	否	String	分组名称 示例值： group_one

UpdateGroupInfo

更新用户组信息

被如下接口引用：UpdateSubAccount

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
GroupId	是	否	Uint64	用户组id 示例值： 15094
Uid	是	否	Uint64	用户id 示例值： 1258042
GroupName	否	否	String	用户组名称 示例值： name
Channel	否	否	Int64	息接收渠道 0:无 1: 短信 2：邮件 3：短信+邮件 示例值： 0

CasProviderItem

cas server 配置信息

被如下接口引用：DescribeCasProvider

名称	必选	允许NULL	类型	描述
Id	是	否	Int64	provider id 示例值： 1
CreateUin	是	否	Uint64	创建账户uin 示例值： 110000000001
OwnerUin	是	否	Uint64	主账户uin 示例值： 110000000001
Name	是	否	String	名称 示例值： name
Desc	是	否	String	描述 示例值： desc
ProviderType	是	否	Int64	provider类型 示例值： 8
Status	是	否	Int64	状态 示例值： 0
ModifyTime	是	否	String	修改时间 示例值： 2019-04-29 21:18:28

名称	必选	允许NULL	类型	描述
CreateTime	是	否	String	创建时间 示例值： 2019-04-29 21:18:28
SAMLMetadata	是	否	String	SAML元数据 示例值： ""
SAMLEntityId	是	否	String	SAML实例id 示例值： ""
SAMLSingleSignOn	是	否	String	SAML登陆跳转 示例值： ""
SAMLSingleLogout	是	否	String	SAML登出跳转 示例值： ""
SAMLKeys	是	否	String	SAML关键字 示例值： ""
Cas	是	否	String	Cas 示例值： ""
CasRoot	是	否	String	cas根地址 示例值： https://cas.yfm13.fsphere.cn/
CasLoginUrl	是	否	String	cas登陆url 示例值： https://cas.yfm13.fsphere.cn/cas/login
CasValidateUrl	是	否	String	cas校验url 示例值： https://cas.yfm13.fsphere.cn/cas/serviceValidate
CasLogoutUrl	是	否	String	cas登出url 示例值： https://cas.yfm13.fsphere.cn/cas/logout
Oauth	是	否	String	oauth配置 示例值： ""

AccountAttributeAndValue

扩展属性值

被如下接口引用：GetGroupList、GetGroupsSubAccount、GetSubsGroup、ListGroups、ListGroupsForConsole、ListMaskedSubAccounts、ListSubAccounts

名称	必选	允许NULL	类型	描述
AttributeName	否	否	String	属性名称 示例值： ""
Attribute	否	否	String	属性 示例值： ""
AttributeId	否	否	Int64	属性id 示例值： ""
ValueId	否	否	Int64	值id 示例值： ""
Uin	否	否	Int64	uin 示例值： 110000000001
Value	否	否	String	值 示例值： ""

错误码

功能说明

如果返回结果中存在 Error 字段，则表示调用 API 接口失败。例如：

```
{
  "Response": {
    "Error": {
      "Code": "AuthFailure.SignatureFailure",
      "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
    },
    "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
  }
}
```

Error 中的 Code 表示错误码，Message 表示该错误的具体信息。

错误码列表

公共错误码

错误码	说明
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。 请在控制台检查密钥是否已被删除或者禁用，如状态正常，请检查密钥是否填写正确，注意前后不得有空格。
AuthFailure.SignatureExpire	签名过期。Timestamp 和服务器时间相差不得超过五分钟，请检查本地时间是否和标准时间同步。
AuthFailure.SignatureFailure	签名错误。 签名计算错误，请对照调用方式中的接口鉴权文档检查签名计算过程。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。

错误码	说明
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

业务错误码

错误码	说明
FailedOperation.PolicyFull	用户策略数超过上限。
InvalidParameter.ParamError	非法入参。
FailedOperation.AccountSettingValueCalculateError	配置值计算异常。
InvalidParameter.RoleNameError	角色名不合法。

错误码	说明
InvalidParameter.ResourceError	策略文档的Resource字段不合法。
InvalidParameter.PolicyIdNotExist	策略ID不存在。
FailedOperation.InAsyncModifyError	数据修改中
ResourceNotFound.URLError	url解析异常。
InvalidParameter.ScopeError	Scope字段不合法。
FailedOperation.PolicyNameInUse	PolicyName字段指定的策略名已存在。
InvalidParameter.OperatePoliciesOverLimit	一次操作策略数过多。
InvalidParameter.EffectError	策略文档的Effect字段不合法。
ResourceNotFound.GroupNotExist	用户组不存在。
InvalidParameter.ActionNotExist	action不存在
InvalidParameter.ActionError	策略文档的Action字段不合法。
FailedOperation.NameAlreadyExist	用户名已存在
FailedOperation.SetLoginRuleFail	设置登录策略失败。
InvalidParameter.AttachmentFull	principal字段的授权对象关联策略数已达到上限。
InvalidParameter.PasswordLengthTooShort	密码太短。
InvalidParameter.NotSupportProduct	CAM不支持策略文档中所指定的资源类型。
InvalidParameter.VersionError	策略文档的Version字段不合法。
InvalidParameter.PolicyIdError	输入参数PolicyId不合法。
FailedOperation.IdentityExist	身份认证失败。
InternalError.SystemError	内部错误。
ResourceNotFound.PolicyIdNotFound	PolicyId指定的资源不存在。
FailedOperation.CheckPasswordError	检查密码失败
ResourceUnavailable.IDPMaxLimit	超过idp最大数量限制。
FailedOperation.SkeyExpired	Skey已过期。
InvalidParameter.PolicyNameError	PolicyName字段不合法。

错误码	说明
InvalidParameter.UserNotExist	用户对象不存在。
InvalidParameter.GroupIdError	GroupId字段不合法。
FailedOperation.Accesskey	操作访问密钥错误
FailedOperation.RefreshTokenError	刷新用户token异常。
FailedOperation.AccountSettingConfigError	账号配置元数据异常。
InvalidParameter.CreateGroupErr	创建用户组失败
InvalidParameter.RoleFull	角色数量达到上限。
InvalidParameter.RoleNotExist	角色不存在。
InvalidParameter.RoleNameInUse	相同名称的角色已存在。
InvalidParameter.UinError	Uin字段不合法。
FailedOperation.SubAccountHasKey	子账号存在密钥。
FailedOperation.SecretIdExist	SecretId已存在。
InvalidParameter.ServiceTypeError	ServiceType字段不合法。
InvalidParameter.PolicyDocumentError	PolicyDocument字段不合法。
FailedOperation.AuthCodeError	授权码异常。
FailedOperation.NoneValue	缺少配置。
UnauthorizedOperation	未授权操作
ResourceNotFound.RecordNotExist	记录不存在
FailedOperation.UnknownAccountSettingKey	未知的账号配置项。
ResourceNotFound.IdentityNotExist	身份不存在。
FailedOperation.UserrAccessTokenError	用户接入token异常。
ResourceNotFound.UserNotExist	用户不存在。
FailedOperation.AccountGroupNameNotMatch	配置组名不匹配。
InvalidParameter.PrincipalError	策略文档的principal字段不合法。
FailedOperation.UnknownAccountSettingGroup	未知的账号配置组。

错误码	说明
InvalidParameter.ConditionError	策略文档的condition字段不合法。
FailedOperation.AddIdentityError	添加认证身份失败。
InvalidParameter.DescriptionLengthOverlimit	Description入参长度不能大于300字节。
InvalidParameter.PolicyDocumentLengthOverLimit	PolicyDocument字段超过长度限制。
InvalidParameter.KeywordError	Keyword字段不合法。
ResourceNotFound.NotFound	资源不存在。
InvalidParameter.StatementError	策略文档的Statement字段不合法。