

访问管理  
产品简介  
产品文档



腾讯云

**【版权声明】**

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

**【商标声明】**

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

**【服务声明】**

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

---

## 文档目录

产品简介

CAM 概述

产品功能

应用场景

使用限制

基本概念

用户类型

## 产品简介

# CAM 概述

最近更新时间：2024-01-23 17:23:14

访问管理（Cloud Access Management, CAM）是腾讯云提供的 Web 服务，主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。

您 [注册腾讯云](#) 时，生成的账号为主账号，拥有该主账号下所有云资源的管理权限。

如您需要其他用户能协助您一起管理账号下的云资源，您可以通过访问管理（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腾讯云资源的权限。

# 产品功能

最近更新时间：2024-01-23 17:23:14

CAM 提供以下功能支持：

## 管理访问权限

可以在主账号里创建子账号，给予账号分配主账号下资源的管理权限，而不需要分享主账号的相关的身份凭证。

## 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某个 COS 存储桶的读权限，而另外一些子账号可以拥有某个 COS 存储对象的写权限等。这里的资源、访问权限、用户都可以批量打包。

## 联合身份

通过访问管理使用您现有的身份验证系统（例如，在您的企业网络中或通过 Internet 身份提供商）获得密码的用户，能够获取对您腾讯云账户的临时访问权限。

## 最终一致性

CAM 目前支持腾讯云的多个地域，通过复制策略数据实现跨地域的数据同步，虽然 CAM 对策略的修改会及时提交，不过跨地域策略同步会导致策略生效延迟；同时，CAM 使用缓存来提高性能，在某些情况下可能增加耗时，在之前缓存的数据过期之前，策略更改可能不会生效。

# 应用场景

最近更新时间：2024-01-23 17:23:14

访问管理的 [使用限制](#)。

## 应用场景

### 针对资源的精细化访问控制

给予用户分配资源管理权限。

场景：您可以在 CAM 中创建用户或角色，为其分配单独的安全证书（控制台登录密码、云 API 密钥等）或请求临时安全证书，供其访问腾讯云资源。您可以管理权限，以控制用户和角色具体可以执行哪些操作和访问哪些资源。

### 企业目录单点登录腾讯云

已具有腾讯云外部身份，并且这些用户需要访问腾讯云资源。

场景：您可通过 CAM 使用您现有的身份验证体系向员工以及服务提供腾讯云服务和资源的访问权限。腾讯云支持基于 SAML 2.0（Security Assertion Markup Language 2.0）的联合身份验证来实现与企业内网账号的互通，[单击此处](#)了解更多详情。

### 账户安全升级，使用二次身份校验

需要给予用户提供用户名和密码之外再额外增加的一层保护。

场景：支持2种校验方式：MFA 设备校验（分为硬件 MFA 设备校验和虚拟 MFA 设备校验）、手机验证码校验。根据设置状态，可能需要在登录和进行敏感操作前提供有效的六位安全码来证实身份和环境安全可靠。

# 使用限制

最近更新时间：2024-01-23 17:23:14

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
一个主账号中的角色数	1000
一个子账号可加入的用户组数	10
一个协作者可协作的主账号数	10
一个用户组中的子账号数	100
未实名认证主账号24小时内创建子账号数	10
一个主账号可创建的自定义策略数 <sup>1</sup>	1500
直接关联到一个用户、用户组或角色的策略数 <sup>2</sup>	200
一个策略语法最大字符数	6144

## 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、用户组或角色的策略数包含 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。

# 基本概念

最近更新时间：2024-01-23 17:23:14

在使用访问管理 CAM 之前，您首先需要了解一些相关概念，例如主账号、子账号、子用户、协作者、用户组等。了解这些概念可以帮助您更好地理解和使用访问管理产品。

## 主账号

用户申请腾讯云账号时，系统会创建一个用于登录腾讯云服务的主账号身份。主账号是腾讯云资源使用计量计费的基本主体。主账号默认拥有其名下所拥有的资源的完全访问权限，可以创建子账号并为子账号设置权限。

## 子账号

子账号为您在腾讯云中创建的实体，有确定的身份 ID 和身份凭证。分为子用户、协作者以及消息接收人。其中子用户和协作者的区别在于子用户完全归属于主账号，而协作者为之前已经注册的腾讯云主账号。即协作者可以有两个身份，一个为自身账号的主账号，也可以切换为对应主账号的协作者。具体可参考 [用户类型](#)。

## 管理员用户

管理员用户是拥有 `AdministratorAccess` 策略权限的子账号，由主账号或者其他管理员用户创建，可以管理您腾讯云账号内所有的用户及其权限、财务相关的信息、以及云服务资产。

## 用户组

用户组是多个相同职能的用户（子账号）的集合。您可以根据业务需求创建不同的用户组，为用户组关联适当的策略，以分配不同权限。

## 角色

CAM 的角色可以理解为一种虚拟用户，与子账号、协作者或消息接受者这类实体用户不同。角色同样可被授予策略。

角色可以是任一腾讯云账号代入，并不是唯一地与某个账号绑定关联。角色没有关联的持久证书（密码或访问密钥），主账号仅在申请角色时需要使用持久证书，在用户担任某个角色时，则会动态创建临时证书并为用户进行相应访问时提供该临时证书，即可通过控制台和 API 两种方式使用角色。

## 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

策略是用于定义和描述一条或多条权限的语法规则。腾讯云的策略类型分为预设策略和自定义策略。



## 预设策略

预设策略由腾讯云创建和管理，是被用户高频使用的一些常见权限集合，如管理员权限（AdministratorAccess）、云服务器全读写权限（QcloudCVMFullAccess）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，可以灵活地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。

# 用户类型

最近更新时间：2024-01-23 17:23:14

CAM 用户为您在腾讯云中创建的一个实体，每一个 CAM 用户仅同一个腾讯云账户关联。您注册的腾讯云账号身份为**主账号**，您可以通过 [用户管理](#) 来创建拥有不同权限的**子账号**协助您。子账号的类型分为 [子用户](#)、[协作者](#) 以及 [消息接收人](#)。

账号类型	主账号	子账号		
		子用户	协作者	消息接收人
定义	拥有腾讯云所有资源，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。	本身拥有主账号身份，被添加作为当前主账号的协作者，则为当前主账号的子账号之一，可切换回主账号身份。	仅拥有消息接收功能。
控制台访问	✓	✓	✓	-
编程访问	✓	✓	✓	-
策略授权	默认已拥有全部策略	✓	✓	-
消息通知	✓	✓	✓	✓