# 访问管理

# 产品简介

# 产品文档

腾讯云

# 文档目录

# 产品简介
# CAM 概述

最近更新时间：2021-07-19 17:57:38

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：2020-04-24 18:01:53

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，给子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：2020-04-22 17:03:24

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

给子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

需要给子用户提供在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：2020-05-26 14:27:01

| 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 |
| 一个主账号可创建的自定义策略数[1] | 1500 |
| 直接关联到一个用户、用户组或角色的策略数[2] | 200 |
| 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：2021-08-03 17:21:43

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范。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。

# 支持 CAM 的产品

最近更新时间：2021-08-23 16:12:41

## 简介

访问管理已经支持对多数腾讯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腾讯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。

> 说明：
> 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。
- 服务角色：当前服务是否支持作为角色载体进行跨服务授权访问其他服务，“✓”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 [1] | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| 弹性伸缩 | 资源级 | ✓ | ✓ | ✓ | - |

| 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 |
| --- | --- | --- | --- | --- | --- |
| 批量计算 | 资源级 | ✓ | ✓ | - | 访问管理指南 |

说明：

[1] 云服务器中 GPU 云服务器、专用宿主机 均已支持使用 CAM。

## 容器

| 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 |
| --- | --- | --- | --- | --- | --- |
| 容器服务 | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| 容器镜像服务 | 资源级 | 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 | ✓ | ✓ [1] | ✓ | 访问管理指南 |
| 文件存储 | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| 云硬盘 | 资源级 | ✓ | ✓ | - | - |
| 云数据迁移 | 服务级 | ✓ | - | - | - |
| 日志服务 | 资源级 | ✓ | - | ✓ | 访问管理指南 |

说明：

[1] 对象存储中 GetService 和 PutBucket 暂未支持标签授权，需要单独进行自定义策略授权。

## 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 VPC [1] | 资源级 | ✓ | ✓ | - | - |
| 专线接入 | 资源级 | ✓ | ✓ | - | - |

说明：

[1] 私有网络中 弹性网卡、NAT 网关、对等连接、VPN 连接、网络流日志 、Anycast 公网加速、云联网、共享带宽包 均已支持使用 CAM。

## CDN 与加速

| 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 |
| --- | --- | --- | --- | --- | --- |
| 全球应用加速 | 资源级 | ✓ | ✓ | - | - |
| 全站加速网络 | 资源级 | ✓ | ✓ | - | - |
| 内容分发网络[1] | 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 |
| --- | --- | --- | --- | --- | --- |
| 云数据库 MySQL | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| 云数据库 MariaDB | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| 云数据库 SQL Server | 资源级 | ✓ | ✓ | - | 访问管理指南 |
| 云数据库 PostgreSQL | 资源级 | ✓ | ✓ | - | - |
| TDSQL MySQL版 | 资源级 | ✓ | ✓ | - | 访问管理指南 |
| 云数据库 Redis | 资源级 | ✓ | - | - | 访问管理指南 |
| 云数据库 MongoDB | 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 |
| --- | --- | --- | --- | --- | --- |
| 数据传输服务 | 资源级 | ✓ | ✓ | ✓ | - |
| 游戏数据库 TcaplusDB | 资源级 | ✓ | ✓ | - | - |
| 数据库智能管家 DBbrain | 资源级 | ✓ | - | - | 访问管理指南 |
| TDSQL-A PostgreSQL 版 | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |

## Serverless

| 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 |
| --- | --- | --- | --- | --- | --- |
| 云函数 | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| Serverless 应用中心 | 资源级 | - | - | ✓ | - |
| Serverless Framework | - | - | - | ✓ | - |

## 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 |
| --- | --- | --- | --- | --- | --- |
| 消息队列 CMQ | 资源级 | ✓ | ✓ | - | 访问管理指南 |
| 消息队列 CKafka | 资源级 | ✓ | - | ✓ | - |
| API 网关 | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |

## 数据处理

| 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 |
| --- | --- | --- | --- | --- | --- |
| 数据万象 | 资源级 | ✓ | - | ✓ | 访问管理指南 |

## 域名与网站

| 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 |
| --- | --- | --- | --- | --- | --- |
| 网站备案 | 服务级 | ✓ | - | - | - |
| SSL证书 | 资源级 | ✓ | - | - | - |

## 数据安全

| 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 |
| --- | --- | --- | --- | --- | --- |
| 密钥管理系统 | 资源级 | ✓ | ✓ | - | 访问管理指南 |

## 安全管理

| 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 |
| --- | --- | --- | --- | --- | --- |
| 安全运营中心 | 操作级 | ✓ | - | ✓ | - |

## 应用安全

| 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 |
| --- | --- | --- | --- | --- | --- |
| Web 应用防火墙 | 操作级 | ✓ | - | - | - |

## 视频服务

| 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 |
| --- | --- | --- | --- | --- | --- |
| 实时音视频 | 资源级 | ✓ | ✓ | - | - |
| 云直播 | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| 云点播 | 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 |
| --- | --- | --- | --- | --- | --- |
| 视频处理 | 服务级 | ✓ | - | ✓ | - |
| 媒体直播 | 操作级 | ✓ | - | - | - |
| 媒体包装 | 操作级 | ✓ | - | - | - |

## 云智大数据平台

| 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 |
| --- | --- | --- | --- | --- | --- |
| 弹性 MapReduce | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| Elasticsearch Service | 资源级 | ✓ | ✓ | - | 访问管理指南 |

## 图像识别

| 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 |
| --- | --- | --- | --- | --- | --- |
| 文字识别 | 服务级 | ✓ | - | - | - |

## 游戏服务

| 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 |
| --- | --- | --- | --- | --- | --- |
| 游戏多媒体引擎 | 资源级 | ✓ | ✓ | - | - |
| 游戏服务器伸缩 | 资源级 | ✓ | ✓ | ✓ | 访问管理指南 |
| 游戏玩家匹配 | 资源级 | ✓ | ✓ | ✓ | - |

## 移动服务

| 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 |
| --- | --- | --- | --- | --- | --- |

| 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 |
| --- | --- | --- | --- | --- | --- |
| 腾讯移动推送 | 资源级 | ✓ | - | - | 访问管理指南 |

## 云通信

| 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 |
| --- | --- | --- | --- | --- | --- |
| 即时通信 IM | 资源级 | ✓ | - | - | - |
| 短信 | 资源级 | ✓ | ✓ | - | - |

## 云资源管理

| 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 |
| --- | --- | --- | --- | --- | --- |
| 标签 | 操作级 | ✓ | - | - | - |
| 资源编排 TIC | 服务级 | - | - | ✓ | - |

## 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 | ✓ | - | ✓ | - |
| 企业组织 | 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 | 资源级 | ✓ | ✓ | ✓ | - |
| 迁移服务平台 | 服务级 | ✓ | - | ✓ | - |