访问管理

产品简介

腾讯云

文档目录

产品简介
CAM 概述

最近更新时间：2023-10-11 14:33:41

访问管理（Cloud Access Management，CAM）可以帮助您安全、便捷地管理对腾讯云服务和资源的访问。您可以使用 CAM 创建子用户、用户组和角色，并通过策略控制其访问范围。CAM 支持用户和角色 SSO 能力，您可以根据具体管理场景针对性设置企业内用户和腾讯云的互通能力。
您最初创建的腾讯云主账号，拥有整个账号全部腾讯云服务和资源的完全访问权限，建议您保护好主账号的凭证信息，日常使用子用户或角色进行访问，并开启多因素校验和定时轮换密钥。

产品功能

最近更新时间：2023-04-27 17:32:08

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，例如：您可以创建一个存储桶，在该存储桶上设置一组读权限子账号、一组写权限子账号以及一组管理权限子账号。设置完成后，您可以批量将要授权的用户添加到对应的子账号中，并将相应的子账号分配给对应的访问权限。

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

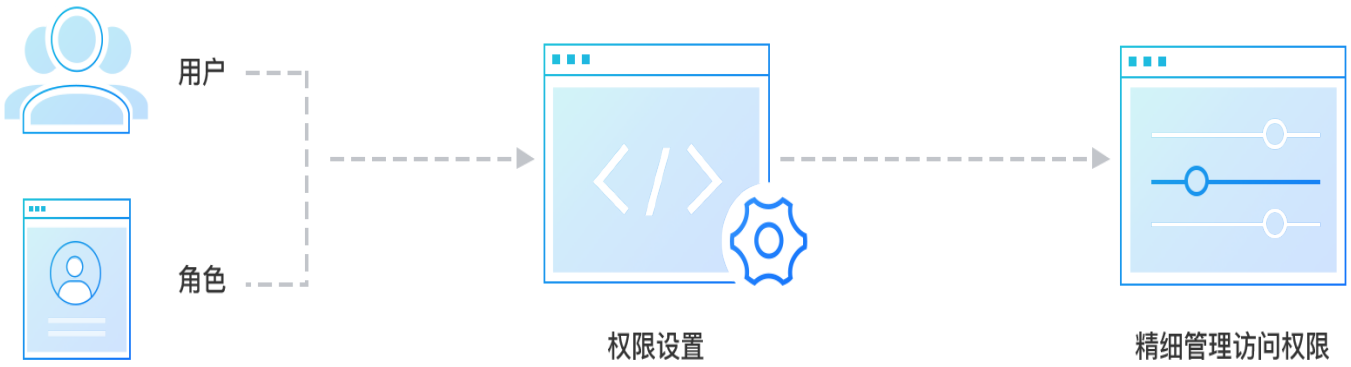
CAM 目前支持腾讯云的多个地域，通过复制策略数据实现跨地域的数据同步，虽然 CAM 对策略的修改会及时提交，不过跨地域策略同步会导致策略生效延迟；同时，CAM 使用缓存来提高性能，在某些情况下可能增加耗时，在之前缓存的数据过期之前，策略更改可能不会生效。

应用场景

最近更新时间：2023-05-22 17:42:40

针对资源的精细化访问控制

- **业务类型**：给子用户分配资源管理权限。
- **使用建议**：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。

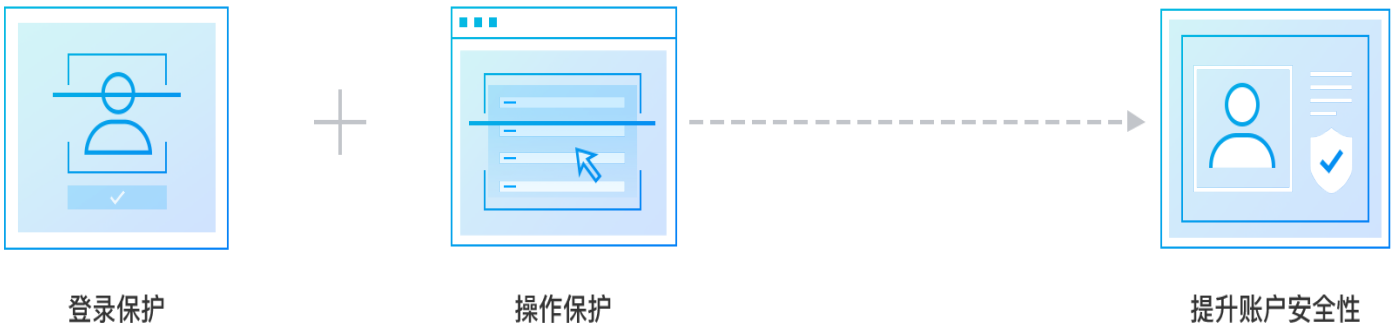


企业目录单点登录腾讯云

- **业务类型**：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。
- **使用建议**：您可通过 CAM 使用您现有的身份验证体系向员工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。

二次身份校验提升账户安全

- **业务类型**：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。
- **使用建议**：支持3种校验方式：微信扫码校验、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进行微信扫码或者提供有效的六位安全码来证实身份和环境安全可靠。



基本概念

最近更新时间：2023-08-25 17:48:21

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、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、企业微信子用户、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，与子用户、协作者或接收消息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，主账号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，用户即可通过控制台和 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。

使用限制

最近更新时间：2023-07-13 14:59:41

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[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	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。

用户类型

最近更新时间：2023-08-25 17:48:21

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 、企业微信子用户、协作者 以及 消息接收人 。

账号类型	主账号	子账号			
		子用户	企业微信子用户	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。	由主账号通过企业微信可见范围导入，完全归属于创建该企业微信子用户的主账号。	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	✔	✔	默认支持控制台登录	✔	–
编程访问	✔	✔	✔	✔	–
策略授权	默认已拥有全部策略	✔	✔	✔	–
消息通知	✔	✔	✔	✔	✔

CAM 之外的安全管理

最近更新时间：2023-08-25 17:48:22

概述

通过访问管理 CAM，可以控制子用户通过腾讯云控制台或者云 API 执行的操作。除此之外，云上产品也有一些资源操作保护的措施，本文仅提供部分示例供您参考。

示例

云服务器 CVM

为保证实例的安全可靠，腾讯云提供两种加密登录方式： 密码登录 和 SSH 密钥对登录 ，其中在配置 Linux 云服务器时您可以选择 SSH 密钥作为云服务器加密登录方式。
根据云服务器操作系统的不同，您可以参考以下文档，在创建云服务器时选择不同的加密登录方式。

- 自定义配置 Windows 云服务器
- 自定义配置 Linux 云服务器

云数据库 MySQL

在云数据库 MySQL 中，需要使用与数据库关联的用户名称和密码来登录。
同时在云数据库 MySQL 实例详情中，选择**数据库管理** > **账号管理**，您可以创建和管理用于登录该数据库的账号。
关于云数据库 MySQL 账号管理的详细说明，请参见 云数据库 MySQL - 创建账号 。

安全组

在访问云服务器 CVM 和云数据库 MySQL 时，可以通过配置安全组来指定可以访问的端口和 IP 等。
关于安全组的详细说明，请参见 云服务器 - 安全组概述 。

总结

如上所述的控制能力并不是 CAM 的一部分，CAM 支持您控制腾讯云产品的方法包括创建或终止 CVM 实例、修改安全组规则等。CAM 可以帮助您控制通过云 API 向腾讯云发起的任务执行请求，或者是在腾讯云控制台的操作。但是，CAM不会帮助您管理诸如登录操作系统 (CVM)、云数据库 MySQL 等任务的安全性。