

Cloud Access Management Product Introduction



Copyright Notice

©2013–2023 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Product Introduction

CAM Overview

Features

Scenarios

Concepts

Limits

User Types

Security Management Beyond CAM

Product Introduction

CAM Overview

Last updated: 2023-08-30 11:54:02

Cloud Access Management (CAM) is a web-based Tencent Cloud service that helps you securely manage and control access to your Tencent Cloud resources.

When you [register with Tencent Cloud](#), the account generated is the root account, which has management permissions for all cloud resources under that account.

If you need other users to assist you in managing the cloud resources under your account, you can create, manage, and terminate users (or user groups) through Cloud Access Management (CAM), and control their access to Tencent Cloud resources using identity management and policy management.

Features

Last updated: 2023-08-30 17:30:24

CAM provides the following features:

Managing access permissions

You can create a sub-account and grant it management permissions for the resources under the root account, without sharing the root account's identity credentials.

Granular permission management

You can assign different access permissions to different resources for different personnel. For instance, you can allow certain sub-accounts to have read access to a specific COS bucket, while other sub-accounts can have write access to a specific COS storage object, etc. Here, resources, access permissions, and users can all be bundled together. For example, you can create a bucket and set a group of sub-accounts with read permissions, a group with write permissions, and a group with management permissions on this bucket. Once set, you can add the users to be authorized in bulk to the corresponding sub-accounts and assign the corresponding access permissions to the respective sub-accounts.

Federated Identity

Users who get passwords through CAM using your existing identity verification system (for example, your enterprise network or through an Internet identity provider) can obtain temporary access permissions to your Tencent Cloud account.

Data integrity

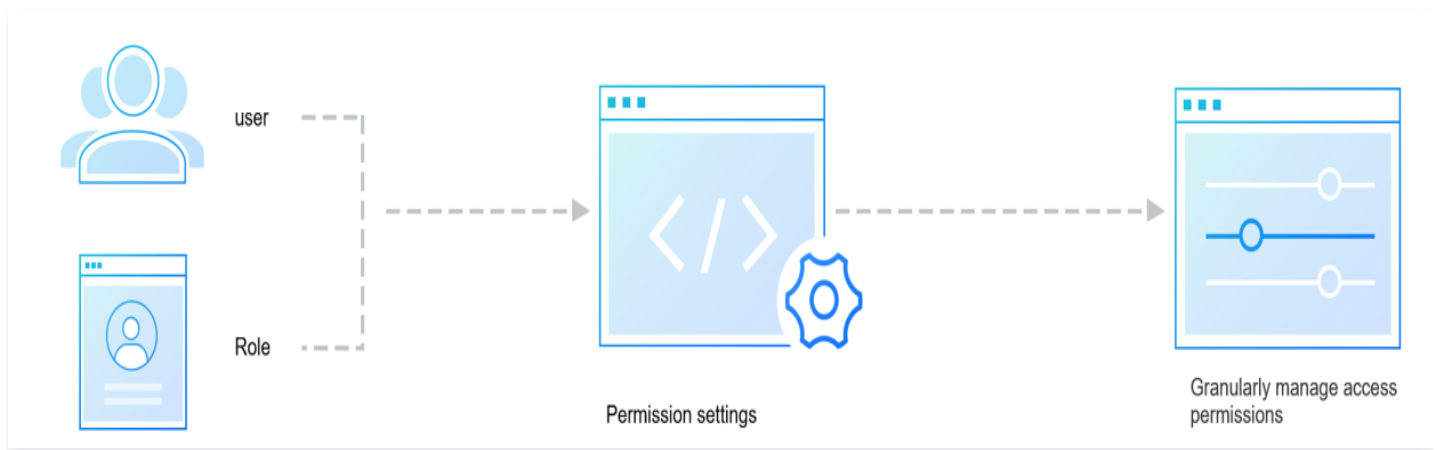
CAM is now available in Tencent Cloud in multiple regions, which allows you to synchronize cross-region data simply through replicating policy data. Although the modified CAM policies will be submitted immediately, the cross-region policy synchronization can result in delayed effects. CAM utilizes cache to improve performance, which may increase the latency in some cases as updates do not take effect until the cache expires.

Scenarios

Last updated: 2023-08-30 17:31:04

Refined Access Control for Resources

- **Business Type:** Assign resource management permissions to sub-users.
- **Usage Recommendations:** In CAM, you can create users or roles, assign them individual security credentials (console login passwords, cloud API keys, etc.), or request temporary security credentials for accessing Tencent Cloud resources. You can manage permissions to control what actions users and roles can perform and which resources they can access.



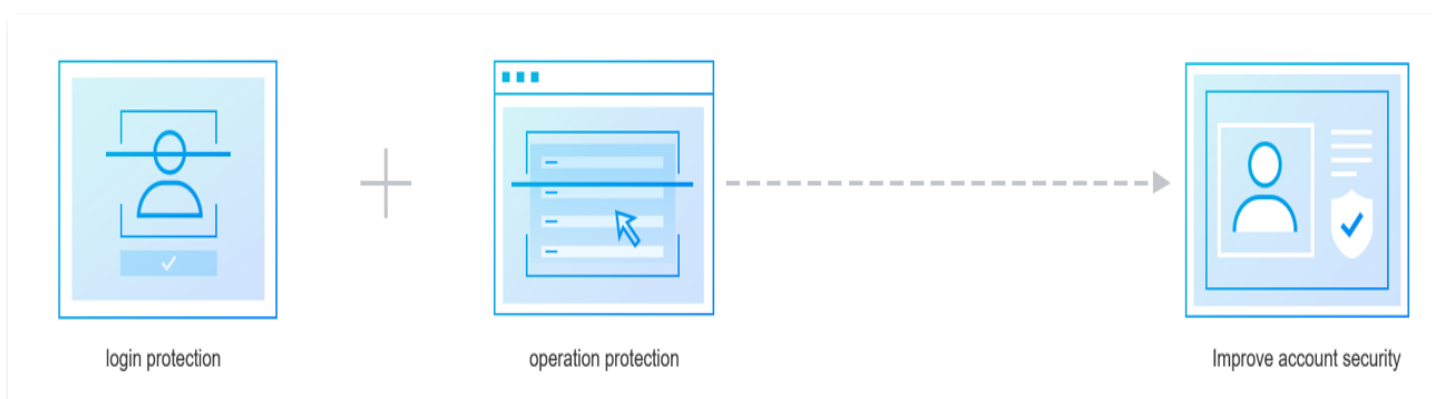
Single Sign-on to Tencent Cloud

- **Business Type:** Users with external Tencent Cloud identities who need to access Tencent Cloud resources.
- **Usage Recommendations:** You can use CAM to provide your employees with access to Tencent Cloud services and resources using your existing identity authentication system. Tencent Cloud supports SAML 2.0 (Security Assertion Markup Language 2.0) based federated identity authentication to achieve interoperability with enterprise intranet accounts. Click [here](#) for more details.



Enhancing Account Security through Multi-factor Authentication

- **Business Type:** Additional layer of protection is required for sub-users beyond username and password.
- **Usage Recommendations:** Supports three verification methods: WeChat QR code verification, MFA device verification (including hardware MFA device verification and virtual MFA device verification), and mobile verification code. Depending on the settings, you may need to scan a WeChat QR code or provide a valid six-digit security code to confirm your identity and ensure a secure environment before logging in or performing sensitive operations.



Concepts

Last updated: 2023-08-30 17:34:46

Before utilizing Cloud Access Management (CAM), it is essential to familiarize yourself with some related concepts such as root accounts, sub-accounts, and user groups. Understanding these concepts will aid in your comprehension and effective use of the access management product.

Root account

Upon application for a Tencent Cloud account, the system generates a root account identity for logging into Tencent Cloud services. This root account serves as the fundamental entity for resource usage measurement and billing within Tencent Cloud. By default, the root account possesses full access rights to all resources under its name and has the ability to create sub-accounts and assign permissions accordingly.

Sub-account

A sub-account is an entity created within Tencent Cloud, possessing a distinct identity ID and credentials. Sub-accounts can be categorized into sub-users, WeCom sub-users, collaborators, and message recipients. The difference between sub-users and collaborators lies in the fact that sub-users are entirely under the root account, while collaborators are previously registered Tencent Cloud root accounts. In other words, a collaborator can have two identities: one as the root account of its own and the other as a collaborator of the corresponding root account. For more details, refer to [User Types](#).

Admin User

An admin user is a sub-account with the permissions of the `AdministratorAccess` policy. It is created by the root account or another admin user and can manage all users and their permissions, financial information, and Tencent Cloud service assets under your Tencent Cloud account.

User group

A user group is a collection of users (sub-accounts) with similar functions. Based on business requirements, you can create various user groups and associate them with appropriate policies to assign different permissions.

Role

A role in CAM can be understood as a type of virtual user, distinct from entity users such as sub-users, collaborators, or message recipients. Roles can also be granted policies. A role

can be assumed by any Tencent Cloud account and is not exclusively associated with a specific account. Roles do not have associated persistent credentials (passwords or access keys). The root account only needs to use persistent credentials when applying for a role. When a user assumes a role, the root account dynamically creates temporary credentials and provides them to the user for corresponding access. Users can use roles through both the console and API.

Permission

Permissions are used to allow or deny specified operations or access to specified resources under specified conditions. By default, a root account is the resource owner and has full access to all resources under the account, while a sub-account does not have access to any resources. Resource creators does not automatically possess access to resources they created and needs be authorized by the resource owner.

Policies

A policy is a syntactical standard used to define and describe one or more permissions. Policies in Tencent Cloud are categorized into preset policies and custom policies.

- **Preset Policies**

Preset policies are created and managed by Tencent Cloud, encompassing a collection of commonly used permissions that are frequently accessed by users, such as Administrator Access (AdministratorAccess), Full Read/Write Access to Cloud Servers (QcloudCVMFullAccess), and so forth. These policies have a broad operational scope and coarse granularity. As system presets, these policies cannot be edited by users.

- **Custom Policy**

A set of permissions, finely crafted by the user, that describes resource management. It allows for granular permission division and can flexibly meet the user's differentiated permission management needs. For instance, a policy can be associated with a database administrator, granting them the authority to manage cloud database instances, but not cloud server instances.

Limits

Last updated: 2023-08-30 17:42:10

Limit	Limit Value
The number of user groups within a primary account	300
The number of sub-accounts within a primary account	1000
The number of roles within a primary account	1000
The number of user groups a sub-account can join	10
The number of root accounts a collaborator can work with	10
The number of sub-accounts within a user group	100
The number of sub-accounts created within 24 hours by an unverified primary account	10
The number of custom policies a primary account can create ¹	1500
The number of policies directly associated with a user, user group, or role ²	200
Maximum character count for a policy syntax	6144

Note

1. The number of custom policies a root account can create, including COS custom policies. If you encounter a **limit exceeded for custom policy count (up to 1500)** message and the number of CAM custom policies has not reached the limit, you can go to the [COS Bucket List - Console](#), click on the bucket name to enter the Permission Management to check if the number of ACLs (Access Control Lists) has exceeded the limit.
2. The number of policies directly associated with a user, user group, or role, including COS custom policies. If you encounter a **policy association failure** message and the number of associated policies in CAM has not reached the limit, you can go to [COS Bucket List - Console](#), click on the bucket name to enter the Permission Management to check if the number of ACLs (Access Control List) has exceeded the limit.

User Types

Last updated: 2023-08-31 16:22:43

A CAM user is an entity you create within Tencent Cloud, each associated exclusively with a single Tencent Cloud account. Your registered Tencent Cloud account is the **primary account**, and you can create **sub-accounts** with varying permissions to assist you through [User Management](#). The types of sub-accounts include [sub-users](#), WeCom sub-users, [collaborators](#), and [message recipients](#).

Account Type	Root account	Sub-account			
		Sub-user	WeCom Sub-user	Collaborator	Message Recipients
Description	Owns all Tencent Cloud resources, and can access any of the resources. It is not advisable to use the root account for resource operations. Instead, create a sub-account and assign policies based on the principle of least privilege. Operate your cloud resources using a sub-account with limited	Created by the root account, and fully belongs to the root account that created the sub-user.	Imported by the root account through the WeCom visibility range, it is fully owned by the root account that created this WeCom sub-user.	When a root account is added as a collaborator of the current root account, it becomes one of the sub-accounts of the current root account. The account can be switched from collaborator back to root account.	Only has message receiving capabilities

	permission scope.				
Query via console	✓	✓	Default support for console login	✓	–
Programming accesses	✓	✓	✓	✓	–
Policy Authorization	Owns all policies by default	✓	✓	✓	–
Message Notification	✓	✓	✓	✓	✓

Security Management Beyond CAM

Last updated: 2023-08-31 16:23:24

Overview

Through Cloud Access Management (CAM), you can control the operations executed by sub-users via the Tencent Cloud Console or Cloud API. In addition to this, there are also some resource operation protection measures for cloud-based products. This document provides only a selection of examples for your reference.

Sample

Cloud Virtual Machine (CVM)

To ensure the security and reliability of instances, Tencent Cloud offers two encrypted login methods: [Password Login](#) and [SSH Key Pair Login](#). When configuring a Linux cloud server, you can choose SSH keys as the encrypted login method for the cloud server.

When creating the CVM, you can refer to the following documents to choose different encrypted login methods based on your CVM operating system.

- [Custom Configuration for Windows CVM](#)
- [Custom Configuration for Linux CVM](#)

TencentDB for MySQL

In TencentDB for MySQL, you need to log in using the username and password associated with the database.

Simultaneously, in the TencentDB for MySQL instance details, select **Database Management** > **Account Management**, where you can create and manage accounts used to log into the database.

For detailed information on managing TencentDB for MySQL accounts, please refer to [TencentDB for MySQL – Creating an Account](#).

Security Group

When accessing Cloud Virtual Machine (CVM) and TencentDB for MySQL, you can specify accessible ports and IPs by configuring the security group.

For a detailed explanation of security groups, please refer to [Cloud Server – Overview of Security Groups](#).

Summary

The control capabilities mentioned above are not part of CAM. CAM supports you in controlling Tencent Cloud products by creating or terminating CVM instances, modifying security group rules, and more. CAM can help you control task execution requests made to Tencent Cloud via the Cloud API, or operations in the Tencent Cloud Console. However, CAM does not assist in managing the security of tasks such as logging into the operating system (CVM), Cloud Database MySQL, and so on.