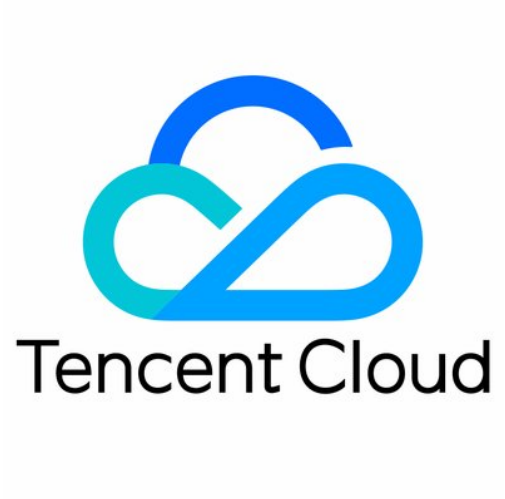
Cloud Access Management

Product Introduction

Product Documentation



Contents

Product Introduction
CAM Overview

Last updated：2024-01-23 17:23:14

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 sign up for Tencent Cloud, the generated account is the root account, which has the management permission for all resources under it.
If you need other users to help you manage the Tencent Cloud resources under your account, you can create, manage, and terminate users (groups) in CAM and use identity and policy management features to control their access to your resources.

Features

Last updated：2024-01-23 17:23:14

CAM provides the following features:

Access Permission Management

A sub-account can be created under a root account and granted the management permissions of the resources there, without having to share the root account's identity credentials.

Refined Permission Management

CAM allows you to use permissions to control who can access what kind of Tencent Cloud resources and services at a granular level. For example, you can grant some sub-accounts read permissions for a specific COS bucket, and other sub-accounts write permissions for a specific COS object. Resources and access permissions can be granted in batches.

Federated Identity

Users who get passwords through CAM by 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.

Use Cases

Last updated：2024-01-23 17:23:14

Go here to see CAM use limits.

Use Cases

Refined access control for resources

Grant resource management permissions to sub-users.
You can create users or roles in CAM and assign them separate security credentials (console login passwords, TencentCloud API keys, etc.) or request temporary credentials for them to access Tencent Cloud resources. You can also manage permissions to control the operations users and roles can perform and the resources they can access.

Single sign-on to Tencent Cloud

Users with external Tencent Cloud roles can access Tencent Cloud resources.
You can use your existing authentication system through CAM to grant your employees and services access permissions to Tencent Cloud services and resources. Tencent Cloud supports federated authentication based on SAML 2.0 (Security Assertion Markup Language 2.0) to implement interconnection with your organizational account systems on a private network. For more information, please click here.

Multi-factor authentication for improved account security

Strengthen your security with an additional layer of protection
We currently support two authentication methods: (hardware/virtual) MFA device authentication and mobile verification code. Depending on the configuration, a user may be required to enter a valid 6-digit authentication code to verify their identity and device environment before logging in or performing sensitive operations.

Basic Concepts

Last updated：2024-01-23 17:23:14

Before using CAM, you need to understand some related concepts first, such as root account, sub-account, sub-user, collaborator, and user group. This helps you better understand and use CAM.

Root Account

When you sign up for a Tencent Cloud account, the system creates a root account identity for you to log in to Tencent Cloud services. Tencent Cloud records your usage and bills you based on the root account. The root account has full access to the resources under it by default and can create sub-accounts and set permissions for them.

Sub-account

A sub-account is an entity you create in Tencent Cloud with a specific ID and credentials. It is divided into sub-user, collaborator, and message recipient. The difference between a sub-user and a collaborator is that a sub-user is fully owned by the root account, while a collaborator is a previously registered Tencent Cloud root account. In other words, a collaborator can have two identities: root account of its own account or collaborator of another root account. For more information, please see 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 multiple users (sub-accounts) with the same functions. You can create different user groups based on your business needs and associate them with appropriate policies to grant them different permissions.

Role

A role in CAM can be seen as a virtual user, which is different from physical users such as sub-accounts, 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 one single account. Although a root account uses persistent credentials such as a password or access keys when creating a role, the role does not have persistent credentials associated with it. When you assume a role, temporary credentials are created for you to access related resources. Specifically, you can use roles through the console and APIs.

Permission

A permission describes whether to allow or refuse execution of certain operations to access certain resources under certain conditions. By default, a root account is the resource owner and has full access to all resources under it, while a sub-account does not have access to any resources. A resource creator does not automatically possess the access to the created resource and should be authorized by the resource owner instead.

Policy

A policy is a syntax rule that defines and describes one or more permissions. Tencent Cloud policy types include preset policy and custom policy.

Preset policy

A preset policy is a set of some common permissions created and managed by Tencent Cloud that are frequently used by users, such as admin permission (AdministratorAccess) and full access to CVM (QcloudCVMFullAccess). Preset policies cover a wide range of operation objects at a coarse operation granularity. They are preset by the system and cannot be edited by users.

Custom policy

A custom policy is user-defined permission sets that describe resource management in a more refined way. It allows fine-grained permission division and can flexibly meet your differentiated permission management needs. For example, you can associate a policy with a database admin so that the admin has the permissions to manage TencentDB instances but not CVM instances.

Use Limits

Last updated：2024-01-23 17:23:14

Item	Upper Limit
Number of user groups in a root account	300
Number of sub-accounts in a root account	1,000
Number of roles in a root account	1000
Number of user groups that a sub-account can be added to	10
Number of root accounts with which a collaborator can be associated	10
Number of sub-accounts in a user group	100
Number of sub-accounts that a root account with an unverified identity can create every 24 hours	10
Number of custom policies created by a root account[1]	1500
Number of policies directly associated with a user, user group, or role[2]	200
Number of characters in a policy	6144

Note:

1. COS custom policies are counted toward the total number of custom policies created by a root account. If you see a prompt saying that **The number of custom policies exceeds the upper limit (1,500)**, but the number of CAM custom policies has not reached the upper limit, you can go to the bucket list in the COS console, click a bucket name and enter the permission management page to check the number of access control lists (ACLs). The combined total might have reached the upper limit.
2. COS custom policies are counted toward the total number of policies directly associated with a user, user group, or role. If you see a prompt saying **Failed to associate the policy**, but the number of associated CAM policies has not reached the upper limit, you can go to the bucket list in the COS console, click a bucket name and enter the permission management page to check the number of access control lists (ACLs). The combined total might have reached the upper limit.

User Types

Last updated：2024-01-23 17:23:14

CAM users are identities you create in Tencent Cloud. Each CAM user is associated with only one Tencent Cloud account. The Tencent Cloud account you registered is the **root account**. You can also create **sub-accounts** with custom permissions in **Users** to help you manage your Tencent Cloud resources. There are 3 types of sub-account: sub-users, collaborators and message recipients.

Account Types	Root Account	Sub-account		
		Sub-user	Collaborator	Message Recipient
Definition	Owns all Tencent Cloud resources, and can access any of the resources. We strongly recommend against using the root account to manage or operate resources. Instead, create sub-accounts and associate them with policies as required. Use these sub-accounts with limited permissions to work with your cloud resources.	Created by the root account, and fully belongs to the root account that created the 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
Console Access	✔	✔	✔	-
Programming Access	✔	✔	✔	-
Policy Authorization	Owns all policies by default	✔	✔	-
Message Notifications	✔	✔	✔	✔