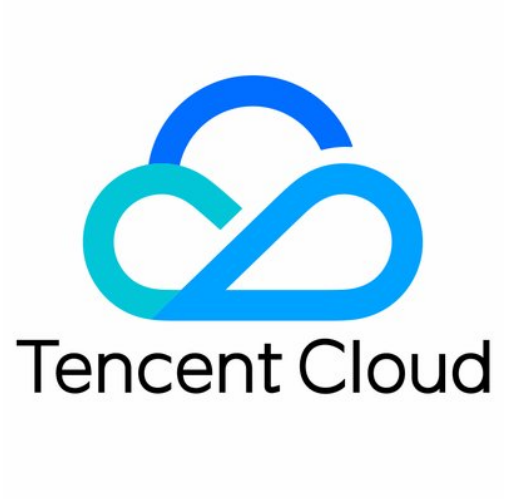
Image Moderation System

Operation Guide

Product Documentation



Contents

Operation Guide
- CAM Authorization Guide
  - Overview
  - Configuring CAM for IMS
    - Enabling CAM for IMS
    - Configuring CAM Permissions for IMS
  - CAM FAQs

Operation Guide
CAM Authorization Guide
Overview

Last updated：2023-12-20 17:27:27

Cloud Access Management (CAM) is a user and permission management system provided by Tencent Cloud for the refined management of access to IMS and its specific APIs. Currently, IMS supports **service-level authorization** and console operations. For more information, see CAM-Enabled Products.

Note:

You can skip this section if you don't need to manage access to IMS resources for sub-accounts. This will not affect your understanding and use of the other sections of the document.

Use Cases

If you have multiple businesses under your Tencent Cloud account which need to be managed separately, you can create sub-users/collaborators in CAM and assign them to the admins of different businesses.

CAM enables you to configure different access permissions for your partners or employees and specify which operations they can perform and which resources they can access, thus implementing least privilege management.

If you have set up an account management system based on the private network, you can connect CAM to your existing authentication system to grant your employees and partners access to Tencent Cloud services and resources.

Configuring CAM for IMS

Enabling CAM for IMS

Last updated：2023-12-20 17:27:27

Creating Sub-user

A root account/admin user can create one or more sub-user accounts for team members and bind permission policies to them. The CAM authorization feature of IMS supports three creation methods: **quick creation, custom creation, and import from WeChat/WeCom**.

Quick creation is easy and fast, but the permission policies that can be bound are relatively fixed.

Custom creation is complex, but it supports batch creation and refined permission policy management.

Import from WeChat/WeCom makes it easier to connect an existing organizational structure or configure permission policies for external members.

For how to create a sub-user, see Creating Sub-user.

Creating Collaborator

An admin user can set the **Tencent Cloud accounts** of other team members as collaborators and grant them access to cloud resources and bind permission policies to them. For detailed directions, see Creating Collaborator.

Configuring CAM Permissions for IMS

Last updated：2023-12-20 17:27:27

Step 1. Log in to the CAM console

After creating a sub-user/collaborator, you can click **Username** on the **User List** management page in the CAM console to disable or enable the console access for the current user in **User Details**.

Note:

The sub-user/collaborator denied access to the console will not be able to log in to the Tencent Cloud console with the current account, but they can still log in to the Tencent Cloud console with their own accounts; in other words, access grant/revocation by the current account does not affect their use of their own Tencent Cloud account.

Step 2. Grant API access (programming access)

You can configure and manage API access keys as instructed in Root Account Access Key Management and Access Key.

Note:

Your API key represents your account identity and granted permissions, **which is equivalent to your login password**. Do not disclose it to others.

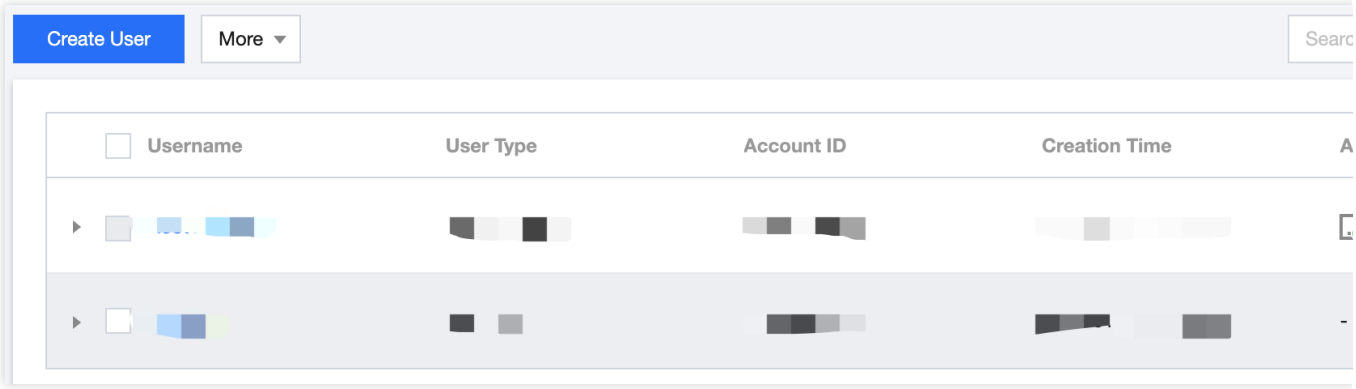
Step 3. Authorize a sub-user/collaborator

Grant access to CMS services

CAM allows you to grant sub-users/collaborators the access permissions of specific CMS services. It can be combined with access method authorization (console/API access) for refined permission management.

Policy authorization process

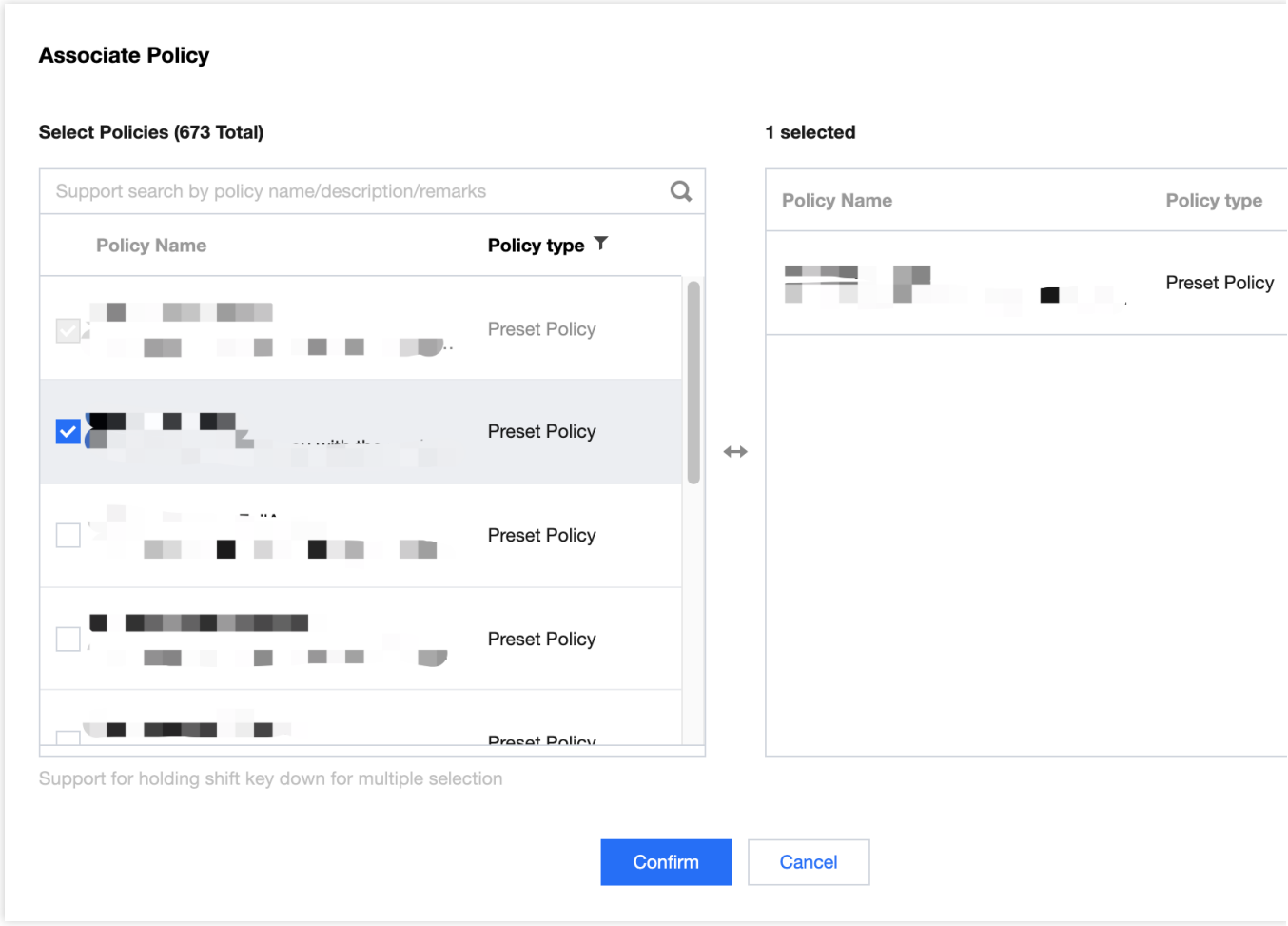
1. Log in to the console with the root account or a sub-user/collaborator with admin permissions and enter the **User List** page.
2. On the **User List** page, select the target sub-user/collaborator and click **Authorize** to pop up the **Associate Policy** page.



3. On the **Associate Policy** page, configure the access permissions of CMS services for the sub-user/collaborator as needed.

Note:

Currently, you can configure **full access/read-only access** to the AMS, VM, IMS, and TMS services under CMS.



4. Click **OK**.

Description of CAM policies for CMS services

The preset policies for CMS services are as listed below:

Service	Preset Policies	Permission Description
TMS	QcloudTMSFullAccess	Full access
	QcloudTMSReadOnlyAccess	Read-Only access
IMS	QcloudIMSFullAccess	Full access
	QcloudIMSFullAccess	Read-Only access
AMS	QcloudAMSFullAccess	Full access
	QcloudAMSReadOnlyAccess	Read-Only access
VM	QcloudVMFullAccess	Full access
	QcloudVMReadOnlyAccess	Read-Only access

Note:

The above preset policies can be used to associate different access permissions of the corresponding CMS services with a sub-user/collaborator. After you assign a preset policy to a sub-user/collaborator as instructed in Authorization Management, the sub-user/collaborator can access or use the corresponding service according to the permissions granted by the policy.

Notes

By default, a root account is the resource owner and has full access to all resources under it, while a sub-user/collaborator 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.

A policy is a syntax rule that defines and describes one or more permissions. There are two policy types: **preset policy** and **custom policy**.

Note:

A preset policy is a set of common permissions that are frequently used by users, such as super admin and full resource access. 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.

A custom policy is a set of user-defined permissions that describes resource management in a more refined way. It allows fine-grained permission division and can flexibly meet your differentiated permission management needs.

You can set user permissions by selecting a policy in the policy list for association, reusing the existing user policy, or adding the user to a group to get the permissions of the group.

For how to create a custom policy, see Creating Custom Policy.

For how to configure a policy for a user/user group, see Authorization Management.

Step 4. Configure and manage CAM

CAM needs to be properly configured and continuously managed to maximize its value. For the security suggestions on the configuration and management of CAM, see Security Setting Policy.

CAM FAQs

Last updated：2023-12-20 17:27:27

How do I set a sub-user/collaborator as admin?

You can grant the sub-user/collaborator the admin permissions by assigning them the preset **AdministratorAccess** policy as instructed in *Configuring Policy for User/User Group*. The policy allows the authorized account to manage all users and their permissions, financial information, and Tencent Cloud service assets under the root account.

How does a sub-user/collaborator get account management permission?

You can grant the sub-user/collaborator the account management permission by assigning them the preset **QcloudCamFullAccess** policy as instructed in Authorization Management. The policy allows you to manage all users and their permissions in the account.
You can also grant the sub-user/collaborator read-only access to CAM by assigning them the preset **QcloudCamReadOnlyAccess** policy.

How does a sub-user/collaborator get the same data viewing permission as the root account?

We recommend you assign the preset **QcloudCamReadOnlyAcces** policy to the sub-user/collaborator as instructed in Authorization Management to grant them read-only access to CAM. When they log in to the console, a user selection box will be displayed on the corresponding pages, and the default option is the current sub-account, which has the same data permissions as the root account.
Note:
You can also grant a sub-user/collaborator the same data viewing permission as the root account by setting them as admin. We recommend you follow the principle of least privilege when doing so.

How do I access the financial information with a root account or financial admin account?

Root account: log in to the Tencent Cloud console and click Billing Center > Bills to view the usage and billing details.
Financial admin account: you need to grant the sub-user/collaborator **financial admin permissions**, console access, and **QCloudFinanceFullAccess** as instructed in Authorization Management, so that they can manage the financial information in the account and view the usage and billing details in Billing Center - Bills in the Tencent Cloud console.

How do I restrict the access IPs of sub-users/collaborators?

You can set login restrictions for sub-users/collaborators in the CAM console, so that they can log in to the Tencent Cloud console only in secure environments. Specifically, you can restrict suspicious logins (from unusual login locations or 30 days after the last successful login) and allow/forbid login from specified IPs. For detailed directions, see Login Restrictions.