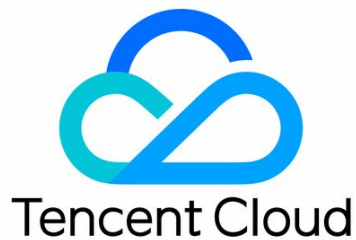


Tencent Cloud Organization Best Practice



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

 Tencent Cloud

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

Best Practice

Centralize management of multiple enterprise accounts' identities and permissions through sub-user authorization

Best Practice

Centralize management of multiple enterprise accounts' identities and permissions through sub-user authorization

Last updated: 2023-08-24 17:50:04

This document introduces how to manage multiple accounts and login permissions for an enterprise through sub-user authorization, thereby enhancing the efficiency of managing members within the organization.

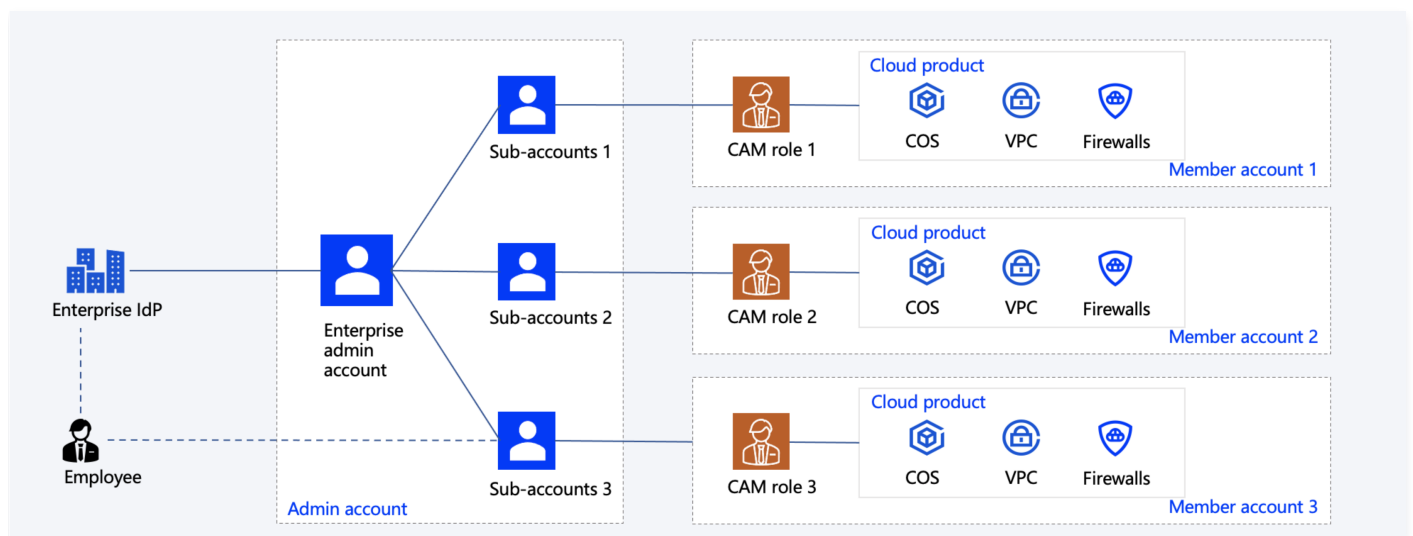
Scenario

Within an enterprise, there are dedicated IT departments or administrators responsible for operations and maintenance in various areas, such as security, networking, and monitoring. When an enterprise has multiple cloud accounts, these IT administrators often need to configure permissions under multiple accounts within the organization to manage network information and security settings for each account.

Customer Challenges

- Configuring permissions across numerous accounts is complex and prone to inconsistency.
- Creating sub-accounts under different accounts increases management complexity and poses risks of account information leakage.
- It is difficult to identify and revoke sub-accounts and permissions of an employee after the employee's permissions change.

Solution Overview



1. The enterprise admin account is integrated with internal accounts, enabling employees to log in to the Tencent Cloud console with single sign-on (SSO).
2. Sub-users are created under the enterprise admin account for employees.
3. Cloud Access Management (CAM) roles are created based on division of responsibilities within the enterprise. Each CAM role is configured to manage multiple accounts with granted access permissions.
4. CAM roles are associated with the member accounts of the enterprise. Employees can then use the associated CAM roles to manage the accounts.
5. Sub-users under the enterprise admin account are granted the permissions to use specific member accounts and CAM roles.
6. Employees can log in to the Tencent Cloud console with SSO to view the member accounts and CAM roles they can use and switch between the accounts.

Practical Application

This document provides an example of using a management account to create a member (user) within a group account and then create a new member login permission (tag_admin) that defines only the tag management permissions.

Next, configure the login permission (tag_admin) for the member (user). Finally, create a group management policy to authorize the sub-user (321) with the permission to log in and manage the member account, thus implementing the management sub-user for the account.

(321) Can only access and manage tag resources within the members (user).

Preparations

1. Please ensure that you have activated a group account and set up a multi-account organizational structure for your enterprise. For more information, see [Create Group Organization](#).
2. Please use the admin account or sub-users of the organization's admin account to perform the operation.

Instructions

1. Log in to the **Organization Console** > [Member Account Management](#).
2. In this example, create a member named "user" within the group account. For detailed instructions, please refer to [Adding Organization Member](#).

The screenshot shows the 'Add member' form with the following fields and options:

- Adding method:** Two tabs: 'Create member' (selected) and 'Invite member'.
- Member name:** A text input field containing 'user'.
- Entity:** Two tabs: 'Current entity' (selected) and 'Other entities'.
- Member finance authorization:** A grid of checkboxes for 'View bills', 'View balance', 'Allocate funds', 'Consolidate bills', 'Invoice', 'Inherit offer', and 'Cost Analysis'.
- Payment mode:** Two tabs: 'Self-pay' (selected) and 'Pay-on-behalf'.
- Department:** A dropdown menu with a 'Create department' link.

Buttons at the bottom: 'OK' and 'Cancel'.

After successfully creating a member, you can view them on the **Organization Management** > [Member account management](#) page, as shown in the image below:

The screenshot shows the 'Member account management' page with a table of members. The table has the following columns: Member name, Member account, Member entity, Directory structure, Member login permission, Member finance, Payment mode, Joining method, Active status, and Operation.

Member name	Member account	Member entity	Directory structure	Member login permission	Member finance	Payment mode	Joining method	Active status	Operation
user				Login permission(1)	Finance management(4)	Self-pay	Create	No	Edit Delete Remove Bind security information

3. Create a new login permission on the **Create login permission** page. In this example, a login permission named "tag_admin" will be created. For detailed instructions, see [Creating Member Login Permission](#) (Bind the preset policy QcloudTAGFullAccess).

Create login permission

Permission name * ✓

Permissions policy * **Select associated policies (3 in total)** ⓘ

tag ✕ 🔍

Policy name

☐ QcloudTAGFullAccess

☐ QcloudTAGReadOnlyAccess

☐ QcloudTIONEReadOnlyAccessContainM... ↔

Selected (0)

Policy name

You can select multiple items by holding down the Shift key.

Please enter descriptions

OK

Close

After successful creation, you can view the settings on the **Organization Management > Login permission settings** page, as shown in the image below:

Login permission settings

ⓘ You can create a login permission and further configure login permission for members in a refined manner on the "Multi-member authorization management" page. Authorized sub-users can only log in to the account within the permission scope. Note that the admin can create up to 20 custom permissions. For more information, see [Documentation](#).

Create login permission

Enter the login permission name 🔍

Login permission name	Login permission type	Description	Modification date	Operation
Admin	Default	Full admin access to member accounts	-	Edit Delete
	Custom	-	2023-08-01 19:48:43	Edit Delete
	Custom	-	2023-05-11 15:48:46	Edit Delete
	Custom	-	2023-06-06 19:36:19	Edit Delete
	Custom	-	2023-06-02 17:07:31	Edit Delete
	Custom	-	2023-06-05 14:19:22	Edit Delete
	Custom	-	2023-05-25 16:24:06	Edit Delete
tag_admin	Custom	-	2023-06-14 19:28:46	Edit Delete
	Custom	-	2023-06-06 16:33:07	Edit Delete
	Custom	-	2023-06-06 16:53:31	Edit Delete

Total items: 11

10 / page

1 / 2 pages

- On the **Configure permission** page, configure the login permission tag_admin for the member user. For detailed instructions, see [Configuring Member Login Permission](#) . (Create the role OrganizationAccesstag_adminMngRole under the member account)

After successful creation, you can view the existing permissions of the member by clicking on the member name **user** in the **Organization Management > Member details** page, and then checking the member details page that opens.

5. Create a group management policy (tag_321) to authorize sub-user (321) with login permissions to manage member accounts (user) with the specified tag. For detailed instructions, please refer to [Authorizing Sub-Users to Log in to Member Accounts](#).
 - Create Group Management Policy (tag_321)

1 Create authorization policy

2 Select sub-user for authorization

Select member

Select member accounts (80 in total) You can select up to 10 members for policy association at a time.

Search by member name/ID

Member name	Account ID
<input checked="" type="checkbox"/> user	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

Selected (1)

Member name	Account ID
user	

Select permission

Login permission

tag_admin

[View login permission](#)

If you select multiple members, the drop-down list will display the intersection of their login permissions.

Enter the policy name

Authorization policy name

tag_123

It can contain up to 128 letters, digits, and symbols (+ = , . @ _ -).

- Granting sub-user (321) the permission to log in and manage the member account with the "user" tag.

← Add member authorization

1 Create authorization policy

2 Select sub-user for authorization

Select sub-user

Select the sub-accounts to be associated (58 in total) Up to five sub-accounts can be associated at a time.

You can enter keywords (separated by space or tab key) to search for sub-account name/ID

Account name	ID
<input checked="" type="checkbox"/> 321	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

Selected (1)

Account name	ID
321	

Complete

Previous

6. Sub-user (321) of the admin account logs in to the member account (user) and accesses the tag resources in the member (user) with the role identity (OrganizationAccesstag_adminMngRole).

Member login

Authorized member list

Add member authorization

1 You can log in to the member account on this page or add sub-users for authorization on the "Add member authorization" page. For more information, see [Documentation](#)

Search by member account ID or sub-acc

Member name	Member account ID	Member login permission	Sub-account ID	Operation
user		1		<div>Log in</div>

Subsequent steps

You can follow the above method to create multiple member accounts and access configurations, grant permissions to multiple members, and achieve unified management of multi-account identities and permissions.