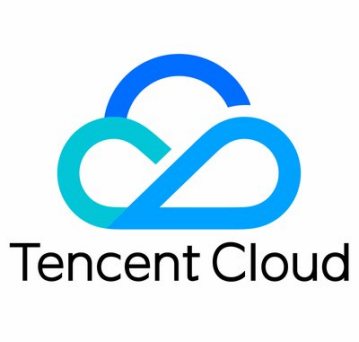
Tencent Cloud Organization Best Practice



Contents

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.

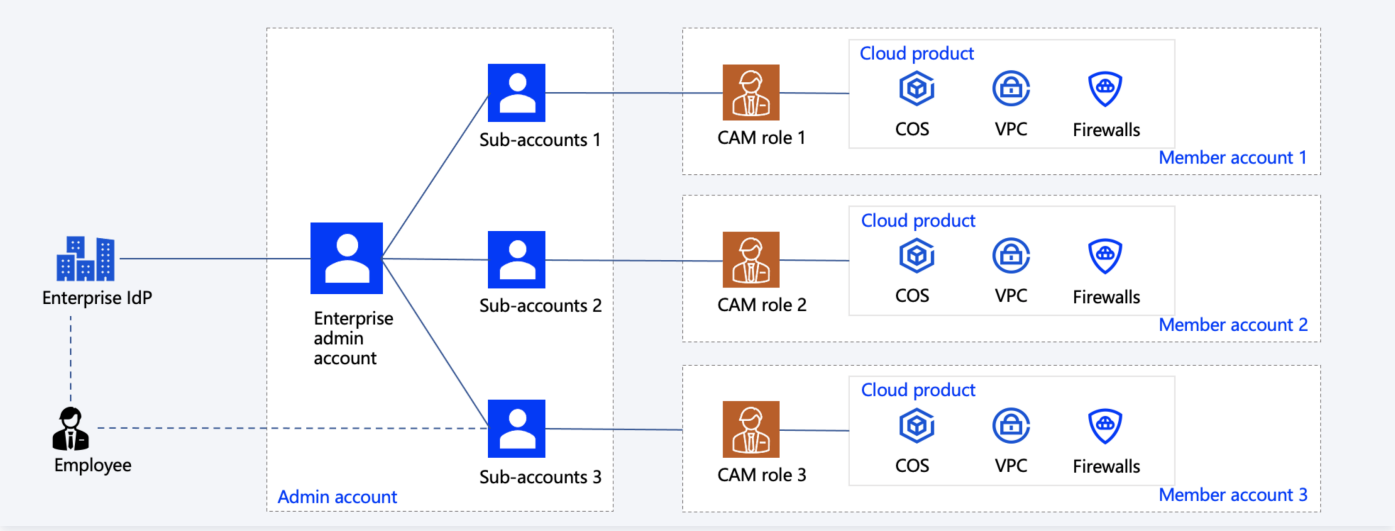
Scenario

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

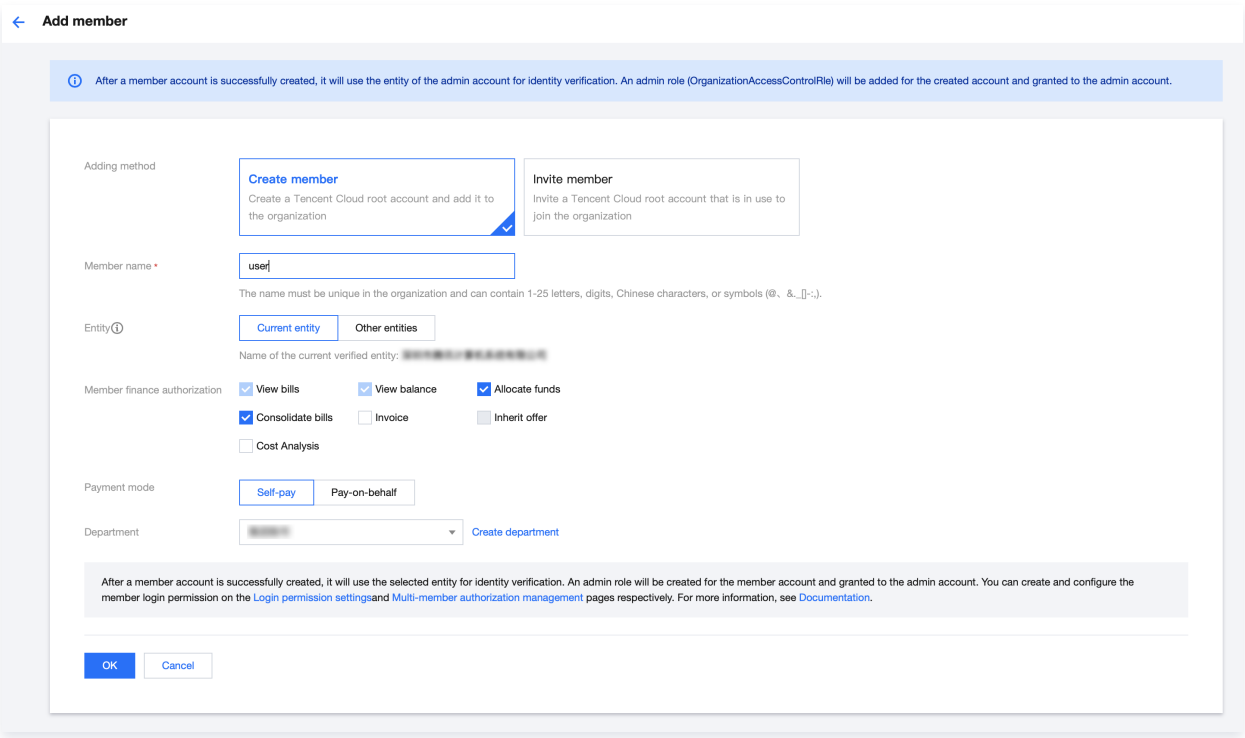
This document provides an example of using a management account to create a member (user) within a group account and then create a new member login permission (tag_admin) that defines only the tag management permissions.
Next, configure the login permission (tag_admin) for the member (user). Finally,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

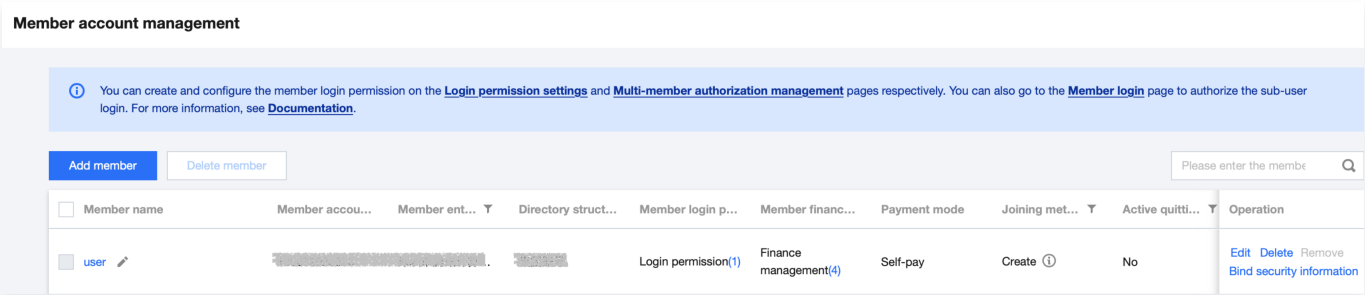
1. Please ensure that you have activated a group account and set up a multi-account organizational structure for your enterprise. For more information, see Create Group Organization.
2. Please use the admin account or sub-users of the organization's admin account to perform the operation.

Instructions

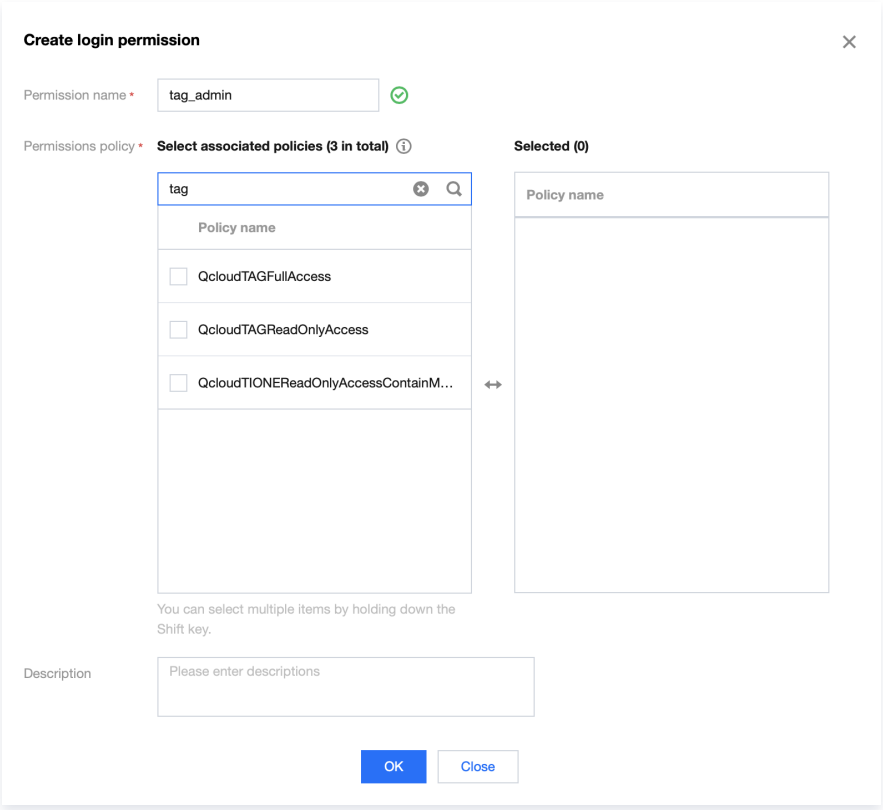
1. Log in to the **Organization Console** > Member Account Management.
2. In this example, create a member named "user" within the group account. For detailed instructions, please refer to Adding Organization Member.



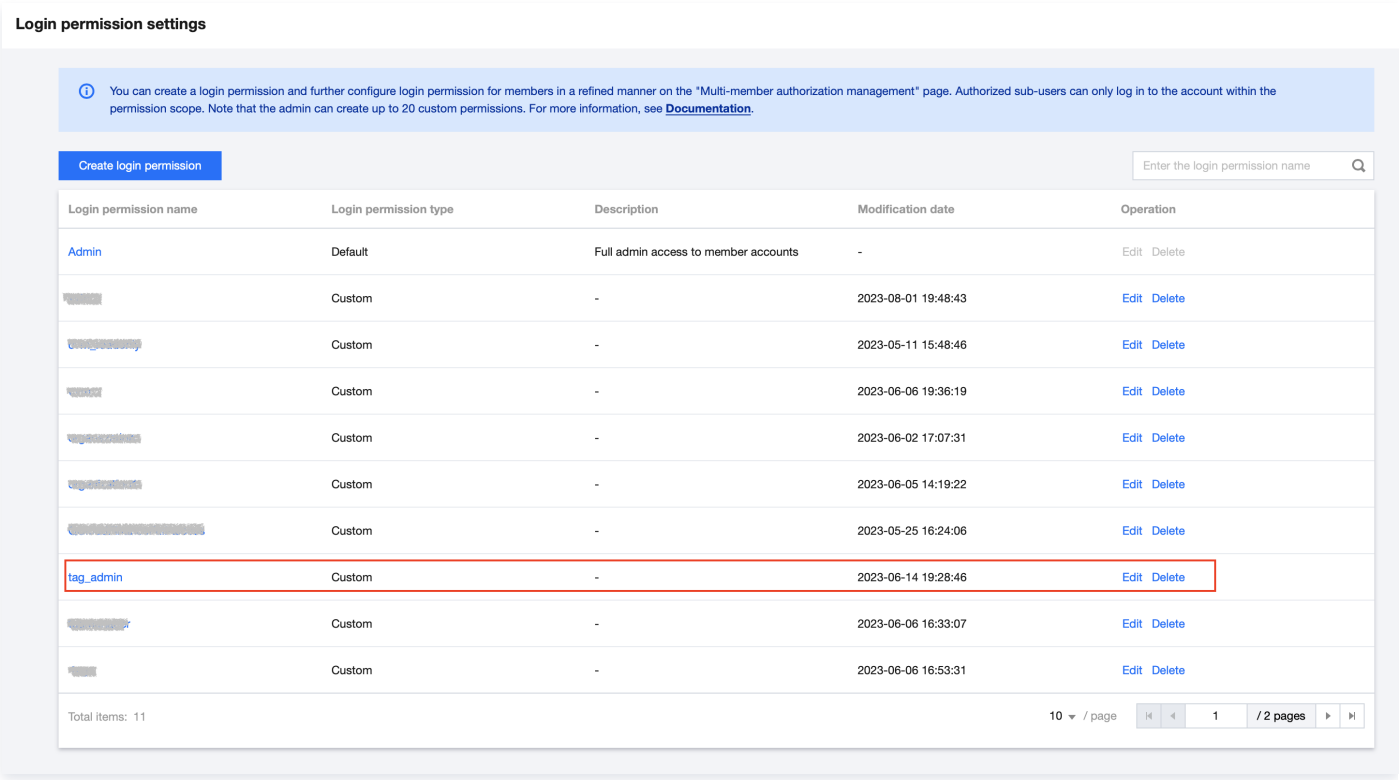
After successfully creating a member, you can view them on the **Organization Management** > Member account management page, as shown in the image below:



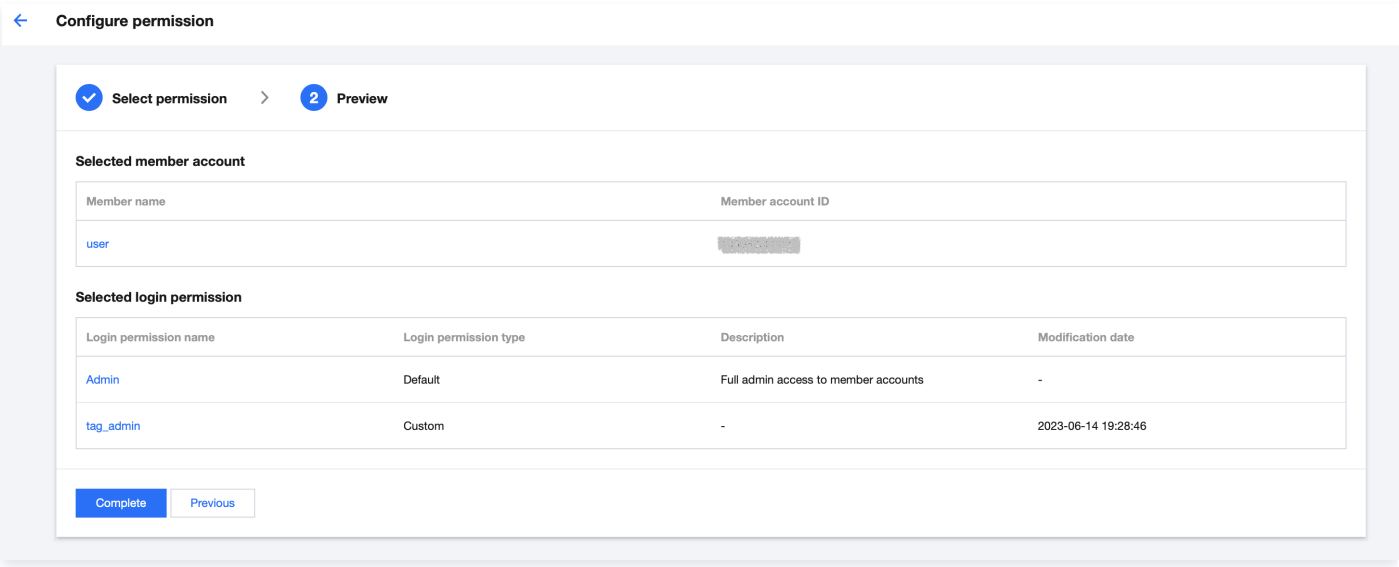
3. Create a new login permission on the **Create login permission** page. In this example, a login permission named "tag_admin" will be created. For detailed instructions, see Creating Member Login Permission (Bind the preset policy QcloudTAGFullAccess).



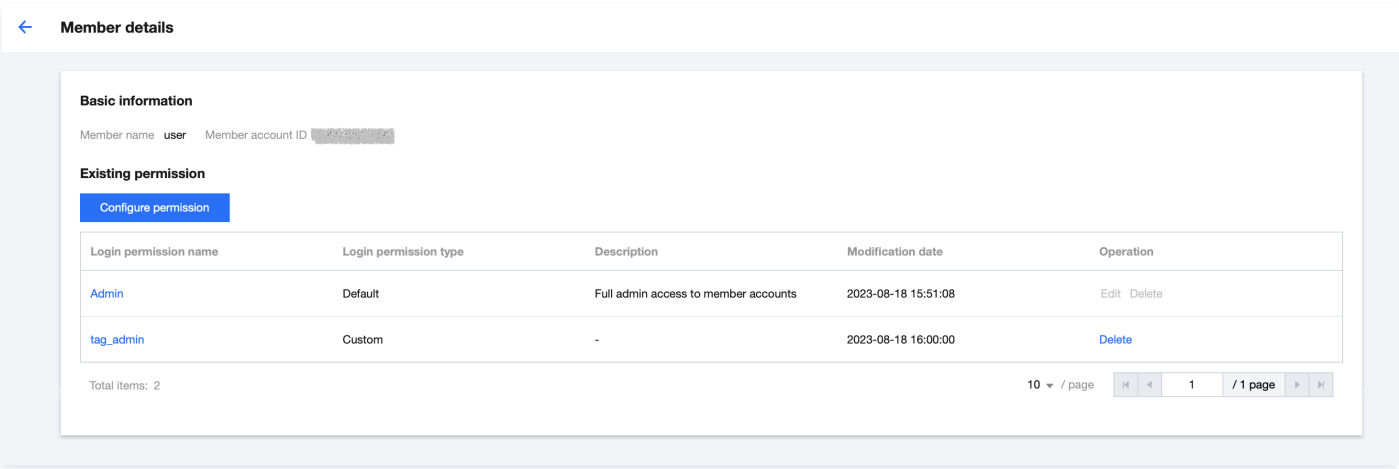
After successful creation, you can view the settings on the **Organization Management** > Login permission settings page, as shown in the image below:



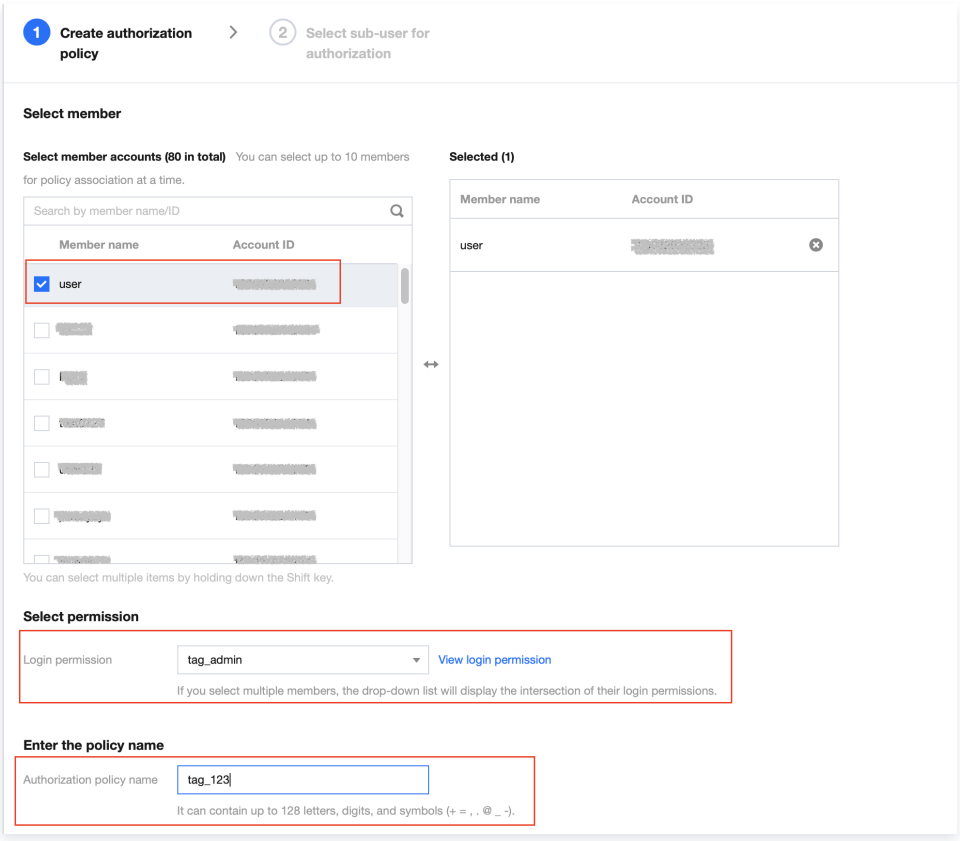
4. On the **Configure permission** page, configure the login permission tag_admin for the member user. For detailed instructions, see Configuring Member Login Permission. (Create the role OrganizationAccesstag_adminMngRole under the member account)



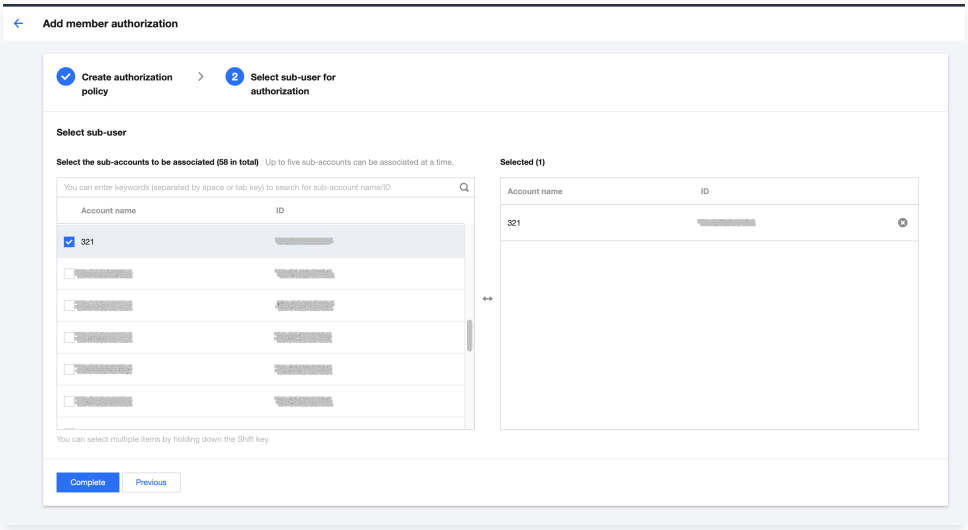
After successful creation, you can view the existing permissions of the member by clicking on the member name **user** in the **Organization Management** > Member details page, and then checking the member details page that opens.



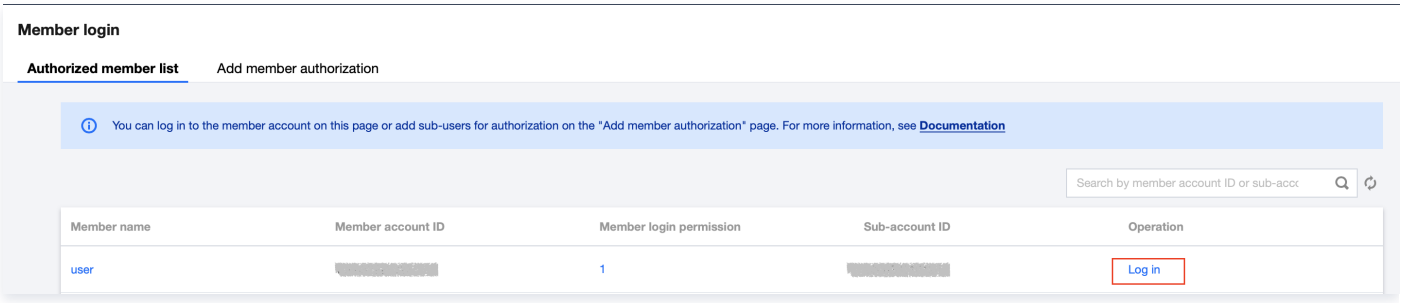
5. Create a group management policy (tag_321) to authorize sub-user (321) with login permissions to manage member accounts (user) with the specified tag. For detailed instructions, please refer to Authorizing Sub-Users to Log in to Member Accounts.
   - Create Group Management Policy (tag_321)



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



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).



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.