Cloud Access Management

Best Practice

Contents

Best Practice

Security Best Practice

Last updated：2024-02-01 19:22:44

Security Settings Overview

In actual application scenarios of enterprises, as business operations expand, an increasing number of resources will be accumulated under each account. Employees from various departments and in different positions will need access to Tencent Cloud, intensifying the enterprise's demand for secure management of resources. This necessitates the establishment of a robust and comprehensive resource control system.

- Employees in different positions have distinct responsibilities, each fulfilling their own roles.
- Employees in the same position may manage different resources.
- The diverse access methods used by employees pose a high risk of resource leakage.
- When an employee leaves the organization, it is necessary to revoke their access permissions to resources.
- The usage of employee accounts needs retrospective analysis and auditing.

Through Cloud Access Management (CAM), you can uniformly allocate account permissions and control account resources in a centralized manner. By adhering to our security setting recommendations, you can establish a secure and comprehensive resource permission management system.

Security Settings Recommendations

1. Accessing Tencent Cloud using a sub-account

Avoid using the primary account's credentials to access Tencent Cloud, and never share these credentials with others. Generally, you should create sub-accounts for all users who need access to Tencent Cloud, and grant these sub-accounts appropriate management permissions. For related settings, please see: User Types.

2. Assign permissions to sub-accounts using groups.

Define groups according to job responsibilities and assign corresponding management permissions to these groups. Then, allocate users to the appropriate groups. In this way, when you modify the permissions of a group, the permissions of the relevant users in the group is changed accordingly. Moreover, when the organizational structure is adjusted, you only need to update the relationship between users and groups. For related settings, please see: User Group.

3. Use different sub-accounts for managing users, permissions, and resources.

- It is advised not to use one sub-account to manage users, permissions, and resources simultaneously. Instead, some sub-accounts should be dedicated to managing users, others to managing permissions, and others to managing other cloud resources.
- It is not recommended to create both a login password for console operations and an access key for API calls for a single CAM user. The specifics are as follows:
  - Programming Access: To access resources via API, simply create an access key.
  - Tencent Cloud Console Access: Simply set a login password to manage resources through the console.

4. Enable Single Sign-On (SSO) for users

Upon enabling SSO, unified identity authentication is carried out for internal enterprise accounts, facilitating access to Tencent Cloud resources using local enterprise accounts.
For related information, see User SSO Overview.

5. Principle of Least Permission

The principle of least permission is a standard security principle. It stipulates that only the minimum permissions necessary to perform a task should be granted, and no unrelated permissions should be given. For instance, if a user is only a user of CDN services, there is no need to grant them access permissions for resources of other services, such as read/write permissions for COS.

6. Configure a Strong Password Policy for CAM Users

You can set password policies through the Cloud Access Management Console, such as password length and required elements in the password. If CAM users are allowed to change their login passwords, they should be required to create strong passwords and regularly rotate their login passwords or access keys.

7. Do not create access keys for the Tencent Cloud primary account.

Access keys are used for API call access, while login passwords are used for console access, both possessing the same permissions. Given that the primary account has full control over its resources, to avoid security risks associated with access key leakage, it is not recommended to create an access key for the primary account and use it for daily operations.
You can create access keys for CAM users, enabling them to carry out daily tasks.
For related operations, please see: Sub-account Access Key Management.

8. Enabling MFA Protection

To enhance account security, we recommend binding MFA to all accounts and enabling login protection and sensitive operation protection for both primary accounts and sub-accounts. For accounts that support email or WeChat login, we strongly recommend enabling MFA for two-factor authentication. Once MFA is enabled, a second verification is required for account login and sensitive operations. For related settings, please see: Set Security Protection for Collaborators, Set Security Protection for Sub-users.

9. Regular rotation of ID credentials

It is recommended that you or CAM users regularly rotate login passwords or cloud API keys. This practice can limit the impact duration in the event of credential leakage.

- For setting up the primary account password, please see: Account Password.
- For setting up a sub-user password, please see: Reset Sub-user Password.

10. Remove unnecessary certificates and permissions.

Remove unnecessary certificates and permissions that are no longer required by users. This minimizes the security risks associated with the leakage of access credentials.

11. Enhancing security through the use of policy conditions

Define conditions as granular as possible for policies, constrain the scenarios in which policies take effect, and enhance security. For instance, restrict users to perform certain operations on specified servers at designated times.
For related settings, see: Element Reference condition.

12. Monitor the operation records of CAM accounts

You can utilize the log recording feature of Tencent Cloud Audit to ascertain the actions performed by CAM users in your account, as well as the resources they have used. The log files will display the time and date of operations, the source IP of the operations, and which operations failed due to insufficient permissions, among other details. For more information, please refer to: Viewing Operation Records.
By adhering to the best security settings recommendations and utilizing these protective mechanisms comprehensively when using Tencent Cloud, a robust and secure resource control system can be established to more effectively safeguard the security of accounts and assets.

More Information

You can download the User Credential Report to obtain the status of all Tencent Cloud sub-accounts and their user credentials, including console login passwords, access keys, and account security settings. This report can be used for compliance audits. For more information, see Download Security Analysis Report.

Authorizing Certain Operations by Tag

Last updated：2024-02-01 19:24:04

Scenario

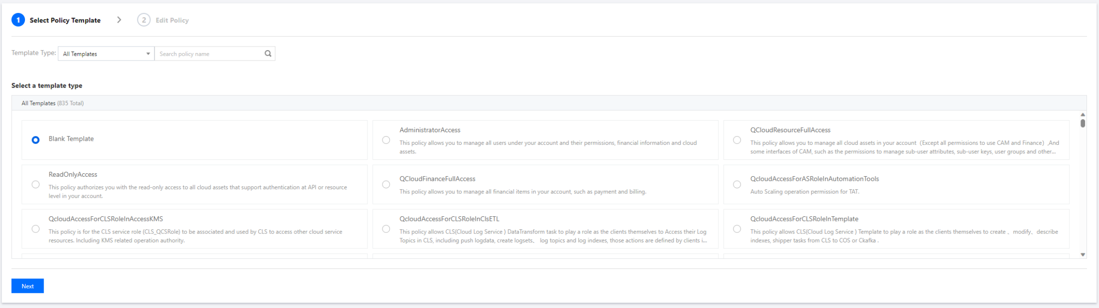
If your organization has purchased a variety of Tencent Cloud resources and manages them through tag-based grouping, you may wish to grant partial interface operation permissions to different team members based on tags. This document presents a typical case to help you understand how to enable sub-accounts to have partial operation permissions for resources under a tag.

Suppose that:

- There is a sub-account, DevA, under the enterprise account CompanyExample.
- The enterprise account CompanyExample has a tag key-value pair named test1&test1.
- The enterprise account CompanyExample intends to grant the sub-account DevA the restart operation permission (cvm:RebootInstances) for CVM resources under the tag test1&test1.

Instructions

1. Log in to the Cloud Access Management Console as the enterprise account CompanyExample.
2. On the **Policies** page, click **Create Custom Policy** > **Create by Policy Syntax**.
3. Under the module type selection, choose the blank template and click **Next** to proceed to the policy editing page.



1 Select Policy Template > 2 Edit Policy

Template Type: All Templates | Search policy name

Select a template type

All Templates (835 Total)

● Blank Template

○ AdministratorAccess
This policy allows you to manage all users under your account and their permissions, financial information and cloud assets.

○ QCloudResourceFullAccess
This policy allows you to manage all cloud assets in your account（Except all permissions to use CAM and Finance）,And some interfaces of CAM, such as the permissions to manage sub-user attributes, sub-user keys, user groups and other...

○ ReadOnlyAccess
This policy authorizes you with the read-only access to all cloud assets that support authentication at API or resource level in your account.

○ QCloudFinanceFullAccess
This policy allows you to manage all financial items in your account, such as payment and billing.

○ QcloudAccessForASRoleInAutomationTools
Auto Scaling operation permission for TAT.

○ QcloudAccessForCLSRoleInAccessKMS
This policy is for the CLS service role (CLS_QCSRole) to be associated and used by CLS to access other cloud service resources. Including KMS related operation authority.

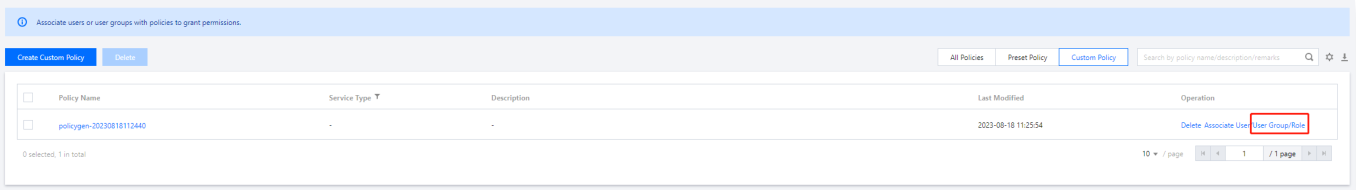
○ QcloudAccessForCLSRoleInClsETL
This policy allows CLS(Cloud Log Service) DataTransform task to play a role as the clients themselves to Access their Log Topics in CLS, including push logdata, create logsets、 log topics and log indexes, those actions are defined by clients i...

○ QcloudAccessForCLSRoleInTemplate
This policy allows CLS(Cloud Log Service) Template to play a role as the clients themselves to create 、modify、describe indexes, shipper tasks from CLS to COS or Ckafka .

4. On the **Edit Policy** page, fill out the following form:
   - Policy name: By default, it is `policygen-current date`. It is recommended that you define a unique and meaningful policy name, such as cvm-RebootInstances.
   - Description: Optional, feel free to compose your own.
   - Policy content: Copy the following content and fill it in. Here, `cvm:RebootInstances` is the name of the interface that needs to be authorized, and `test1&test1` is the tag key and tag value that need to be authorized for operation.

```
   {
"version": "2.0",
"statement": [
   {
      "effect": "allow",
      "action": [
         "cvm:RebootInstances"
      ],
      "resource": "*",
      "condition": {
         "for_any_value:string_equal": {
            "qcs:tag": [
               "test1&test1"
]
}
}
}
]
}
```

5. Click **Complete** to finalize the creation of the policy. The new policy will be displayed on the Policy List page.
6. In the Policy List, search for and locate the policy you just created, then click **Associate User/User Group/Role** under the operation column on the right.

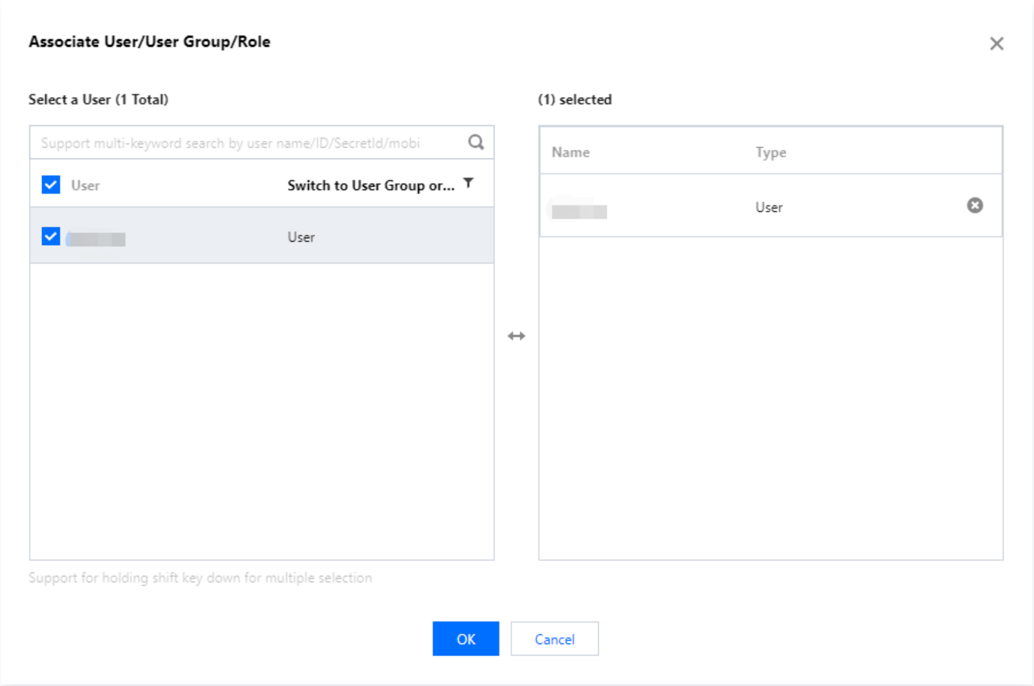


Associate users or user groups with policies to grant permissions.

☐	Policy Name	Service Type	Description	Last Modified	Operation
☐	policygen-20230818112440	-	-	2023-08-18 11:25:54	Delete Associate User/User Group/Role

0 selected, 1 in total

7. In the "Associate User/User Group/Role" window that pops up, search for and select the sub-account DevA, then click **OK** to complete the authorization process.
   The sub-account DevA will now have the permission to restart CVM resources under the tag test1&test1.



Associate User/User Group/Role

Select a User (1 Total)

☑ User	Switch to User Group or...
☑ [redacted]	User

(1) selected

Name	Type
[redacted]	User

Support for holding shift key down for multiple selection

Associated Documents

- If you intend to understand how to establish a relationship between resources and tags, see Manage Tags.
- If you intend to understand how to grant all operation permission for resources under a tag, see Grant Different Sub-accounts Independent Cloud Resource Management Permission.

Supporting Isolated Resource Access for Employees Overview

Last updated：2023-08-31 18:36:42

If your root account has multiple businesses and each business has its own resources, you may want employees from different businesses to be able to see and manipulate different resources when logging in with their CAM sub-accounts.
In this case, you can use two permission setting options in CAM to implement isolated resource access: authorization by resource ID or by tag.

Description

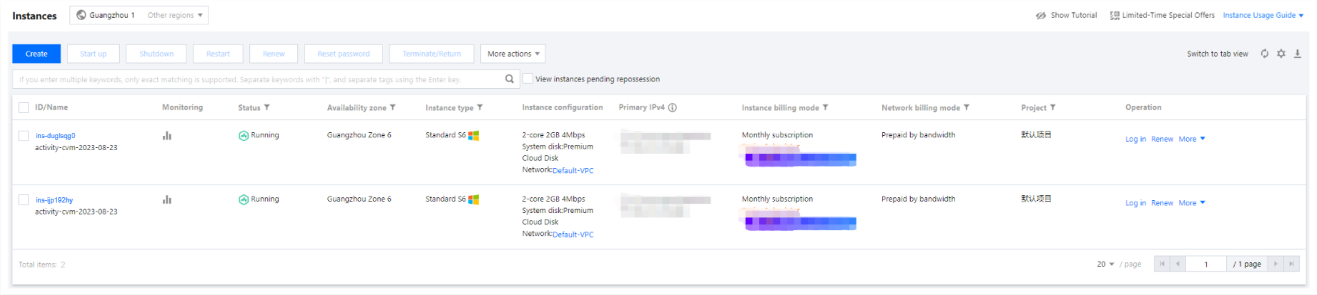
Taking CVM as an example, suppose there are two CVM instances as detailed below:

Resource ID	Image ID	Tag	Project
ins-duglsqg0	img-eb30mz89	game:webpage	webpage
ins-ijp192hy	img-eb30mz89	game:app	app

Create a CAM sub-user named cvmtest01 for the employee and use the two permission setting methods mentioned above to ensure that cvmtest01 can only manage the resource-level interface permissions of ins-duglsqg0.

Expected Result

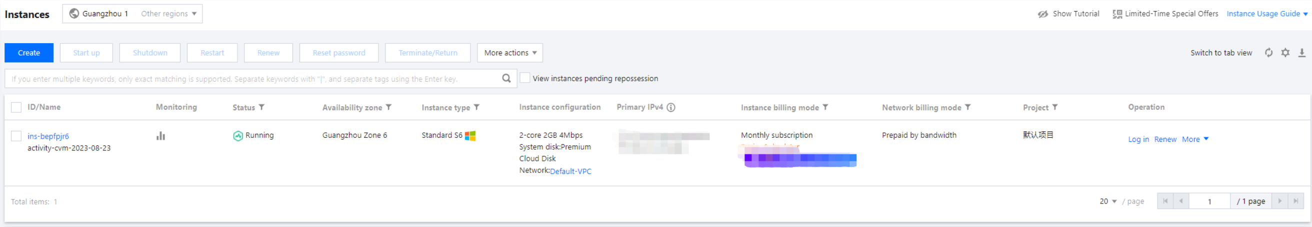
- Viewing the CVM list in the Guangzhou region using the administrator account:


Instances
Guangzhou 1
Other regions
Show Tutorial
Limited-Time Special Offers
Instance Usage Guide
Create
Start up
Shutdown
Restart
Renew
Reset password
Terminate/Return
More actions
Switch to tab view
If you enter multiple keywords, only exact matching is supported. Separate keywords with "|", and separate tags using the Enter key.
View instances pending repossession

ID/Name	Monitoring	Status	Availability zone	Instance type	Instance configuration	Primary IPv4	Instance billing mode	Network billing mode	Project	Operation
ins-duglsqg0 activity-cvm-2023-08-23		Running	Guangzhou Zone 6	Standard S6	2-core 2GB 4Mbps System disk:Premium Cloud Disk Network:Default-VPC	[redacted]	Monthly subscription [redacted]	Prepaid by bandwidth	默认项目	Log in Renew More
ins-ijp192hy activity-cvm-2023-08-23		Running	Guangzhou Zone 6	Standard S6	2-core 2GB 4Mbps System disk:Premium Cloud Disk Network:Default-VPC	[redacted]	Monthly subscription [redacted]	Prepaid by bandwidth	默认项目	Log in Renew More

Total items: 2 20 / page 1 / 1 page

- Using cvmtest01 to view the CVM list in the Guangzhou region:


Instances
Guangzhou 1
Other regions
Show Tutorial
Limited-Time Special Offers
Instance Usage Guide
Create
Start up
Shutdown
Restart
Renew
Reset password
Terminate/Return
More actions
Switch to tab view
If you enter multiple keywords, only exact matching is supported. Separate keywords with "|", and separate tags using the Enter key.
View instances pending repossession

ID/Name	Monitoring	Status	Availability zone	Instance type	Instance configuration	Primary IPv4	Instance billing mode	Network billing mode	Project	Operation
ins-bepfpjr6 activity-cvm-2023-08-23		Running	Guangzhou Zone 6	Standard S6	2-core 2GB 4Mbps System disk:Premium Cloud Disk Network:Default-VPC	[redacted]	Monthly subscription [redacted]	Prepaid by bandwidth	默认项目	Log in Renew More

Total items: 1 20 / page 1 / 1 page

Implementation Method

- Method One: Authorize by Resource ID
- Method Two: Authorize by Tag

Authorization by Tag

Last updated：2024-02-01 19:38:09

Scenario

This guide instructs you on how to grant permissions based on tags, enabling the sub-user cvmtest01 to manage only the resource-level interface permissions of ins-duglsqg0.
View detailed scenarios >>

Policy

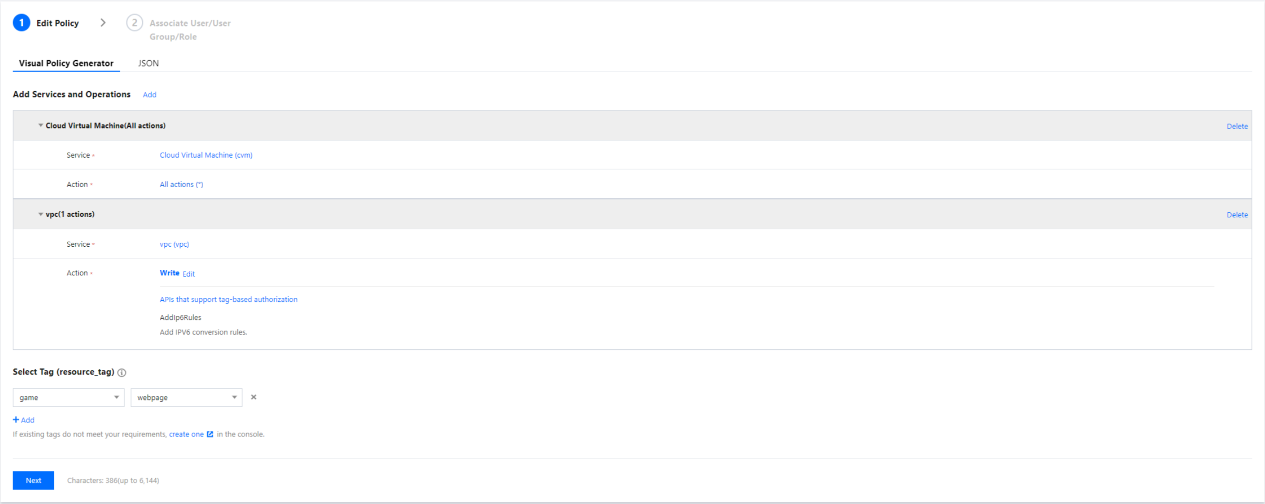
To grant permissions by tag as needed, you can use the following policy content:

```
   {
  "version": "2.0",
  "statement": [
     {
       "effect": "allow",
       "action": [
          "cvm:*",
          "vpc:DescribeVpcEx",
          "vpc:DescribeNetworkInterfaces"
       ],
       "resource": "*",
       "condition": {
          "for_any_value:string_equal": {
             "qcs:resource_tag": [
                "game&webpage"
  ]
}
}
}
  ]
}
```

Instructions

Step 1. Create a policy and configure permissions

1. Log in to the Cloud Access Management Console as an administrator. On the Policies page, create a custom policy by tag (see Creating a Custom Policy by Tag Authorization).



Add Services and Operations

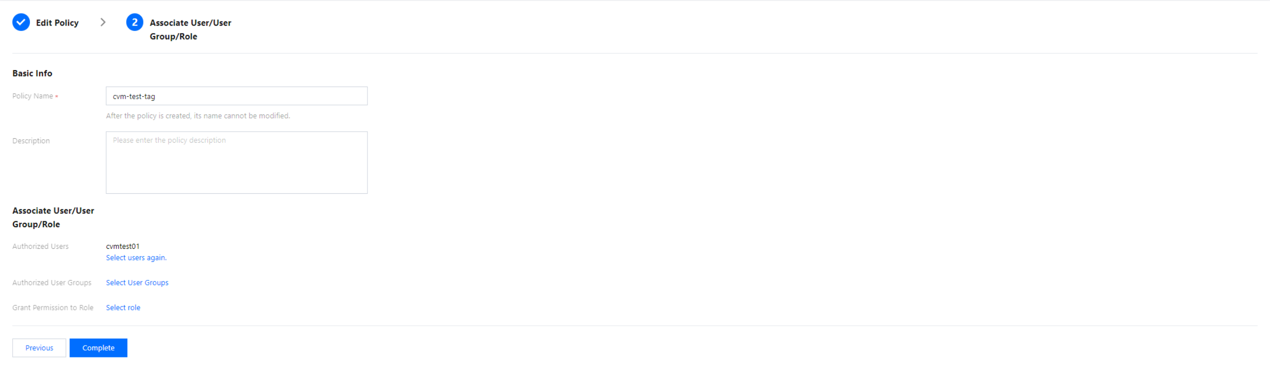
Cloud Virtual Machine(All actions)
Service * Cloud Virtual Machine (cvm)
Action * All actions (*)

vpc(1 actions)
Service * vpc (vpc)
Action * Write
APIs that support tag-based authorization
AddIp6Rules
Add IPV6 conversion rules.

Select Tag (resource_tag)
game webpage

If existing tags do not meet your requirements, create one in the console.

Characters: 386(up to 6,144)



✓ Edit Policy > 2 Associate User/User Group/Role

Basic Info

Policy Name * cvm-test-tag

After the policy is created, its name cannot be modified.

Description Please enter the policy description

Associate User/User Group/Role

Authorized Users cvmtest01 Select users again.

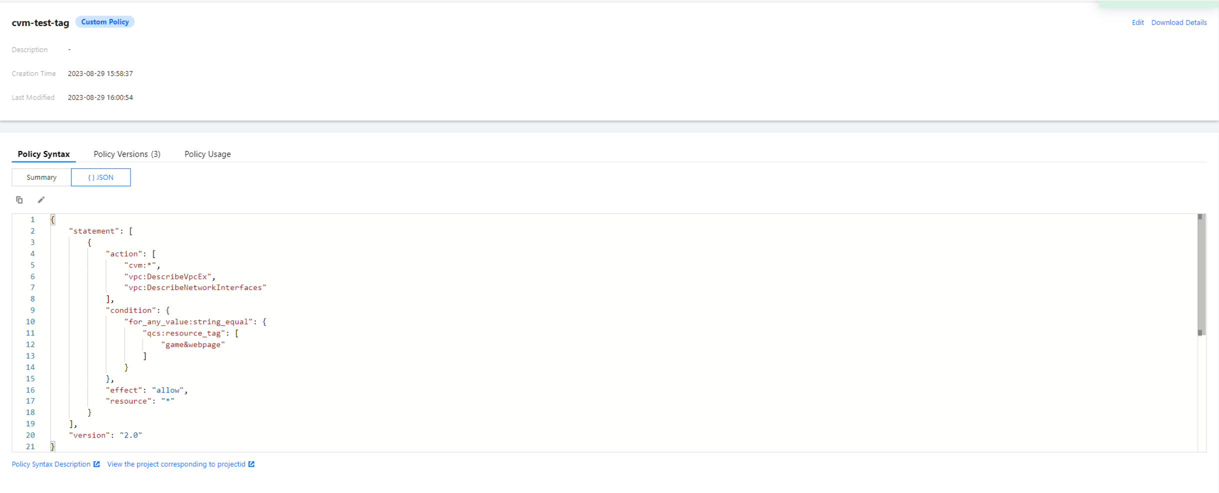
Authorized User Groups Select User Groups

Grant Permission to Role Select role

Previous Complete

- ○ Grant permissions to user: cvmtest01
- ○ Tag Binding: game:webpage
- ○ Required permissions: Full operation permissions for CVM and DescribeVpcEx and DescribeNetworkInterfaces for VPC. (Note: If you are unsure about the other interfaces involved, you can see Grant Permissions by Resource ID – Step 3 for verification and addition)

2. Click **Next** and enter the policy name.
3. Click **Save** to finalize the authorization.



cvm-test-tag Custom Policy

Edit Download Details

Description -

Creation Time 2023-08-29 15:58:37

Last Modified 2023-08-29 16:00:54

Policy Syntax | Policy Versions (3) | Policy Usage

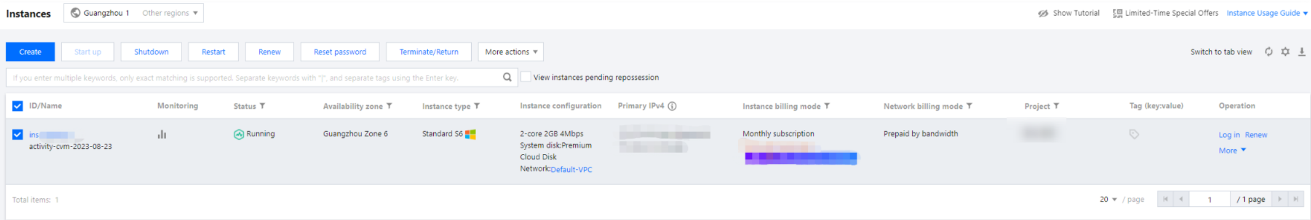
Summary | {} JSON

```
{
    "statement": [
        {
            "action": [
                "cvm:*",
                "vpc:DescribeVpcEx",
                "vpc:DescribeNetworkInterfaces"
            ],
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "game&webpage"
                    ]
                }
            },
            "effect": "allow",
            "resource": "*"
        }
    ],
    "version": "2.0"
}
```

Policy Syntax Description View the project corresponding to projectid

Step 2: Verify the result

The sub-user cvmtest01 should log in to the Cloud Server Console and access the instance list page to achieve the desired effect. At this point, the sub-user cvmtest01 can perform operations such as turning the instance on and off, restarting, renaming, and resetting the password.



Instances Guangzhou 1 Other regions ▾ Show Tutorial Limited-Time Special Offers Instance Usage Guide ▾

Create | Start up | Shutdown | Restart | Renew | Reset password | Terminate/Return | More actions ▾ Switch to tab view

If you enter multiple keywords, only exact matching is supported. Separate keywords with "|", and separate tags using the Enter key. □ View instances pending repossession

☑ ID/Name	Monitoring	Status	Availability zone	Instance type	Instance configuration	Primary IPv4	Instance billing mode	Network billing mode	Project	Tag (key:value)	Operation
☑ ins[redacted] activity-cvm-2023-08-23		Running	Guangzhou Zone 6	Standard S6	2-core 2GB 4Mbps System disk:Premium Cloud Disk Network:Default-VPC	[redacted]	Monthly subscription [redacted]	Prepaid by bandwidth	[redacted]		Log in Renew More ▾

Total items: 1 20 ▾ / page 1 / 1 page

Enterprise Multiple Account Permissions Management Overview

Last updated：2024-02-01 19:38:54

Many enterprises on Tencent Cloud will have multiple primary accounts. The more accounts there are, the more complex the management of accounts and permissions becomes. At this point, enterprise administrators hope to manage resource permissions across accounts to reduce management complexity. If employees need to access multiple primary accounts, they hope to reduce the number of CAM sub-accounts and the frequency of logins.

In response to these scenarios, Tencent Cloud offers three methods for cross-account access and management: Group Accounts, Roles, and Collaborators. The comparison of these three methods is as follows, and you can choose the method that suits your enterprise based on the actual scenario:

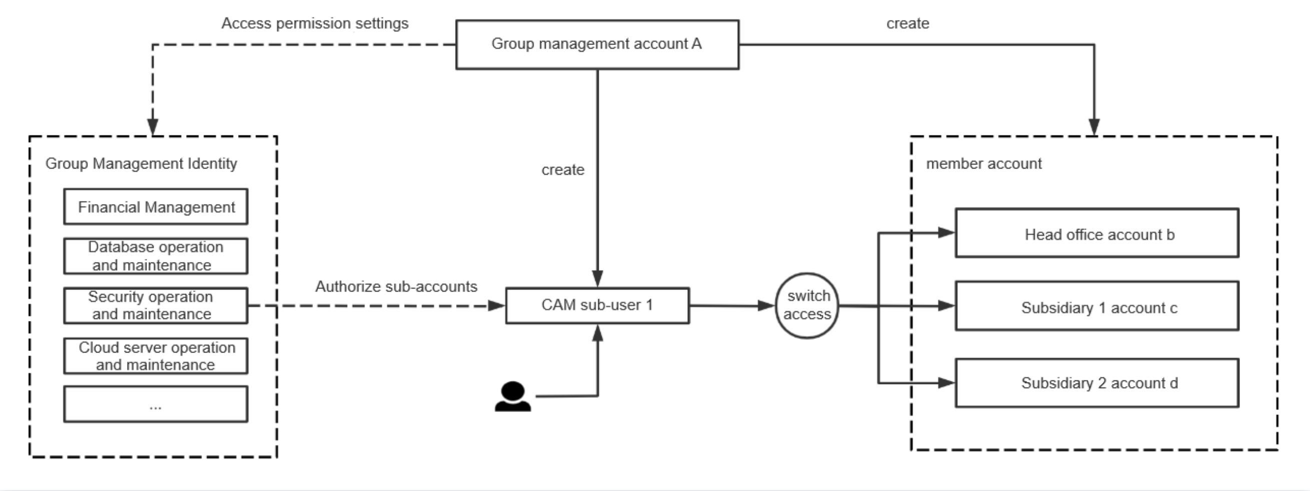
Management Method	Feature Description
Group Account	The graphical interface is easy to operate, but it only supports enterprise accounts with real-name verification within the same group.
Role	A role needs to be created under each managed primary account, resulting in a relatively lengthy operation process.
Collaborator	It only supports primary accounts as collaboration targets

Organization Account

Last updated：2024-02-01 20:51:37

Overview of Tencent Cloud Organization

Tencent Cloud Organization is a multi-account management product on Tencent Cloud designed for group customers. It enables group administrators to centrally manage the Tencent Cloud primary accounts of the group and its subsidiaries, offering capabilities in account, finance, and security management. For more details, see the Tencent Cloud Organization Documentation.
Within Tencent Cloud Organization, the admin account can grant management permissions for multiple created member accounts to a CAM sub-account simultaneously. Once authorized, the CAM sub-account can log in once and select members to manage multiple member accounts.


Access permission settings
Group management account A
create
Group Management Identity
Financial Management
Database operation and maintenance
Security operation and maintenance
Cloud server operation and maintenance
...
create
Authorize sub-accounts
CAM sub-user 1
switch access
member account
Head office account b
Subsidiary 1 account c
Subsidiary 2 account d

Scenario

Assume that a certain group has Account A and Account B on Tencent Cloud, and chooses Account A as the admin account to activate the account management product. The group has Subsidiary 1 and Subsidiary 2, each with Account C and Account D respectively. There is a security administrator, Employee M, within the group who intends to concurrently manage the accounts of the group and its subsidiaries.
At this point, the group's admin account can create CAM Sub-user 1 for Employee M and grant security operation permissions for Accounts B, C, and D. After logging in to the Tencent Cloud Console through CAM Sub-user 1, the employee can switch between different member accounts to perform related security operations, eliminating the need to create a CAM sub-user under each account separately.

Instructions

Add permission

1. The admin account logs in to the **Tencent Cloud Organization** Console and navigates to the Access Permission Settings page.
2. Establish a model to manage all members, such as network operations, security operations, cloud server operations, financial administrators, etc.
   For detailed operations, see Managing Access Permissions.
3. In Member Account Management, click **Add Member**, select **Create Member**, and choose the required permissions. For detailed operations, see Add Organization Members.
4. Once the member is successfully created, grant the sub-user the permission to log in to the member through the **Member Account Management** list > **Login Account**.
   For detailed operations, see Authorize Access to Member Account.

Logging in as a Sub-User

Log in to the **Tencent Cloud Organization Console** as a CAM sub-user, go to Member Account Management, select the members and access permissions you need to manage, and click **Login Account** in the operation column. This allows the sub-user to log in to the member console and perform management operations.

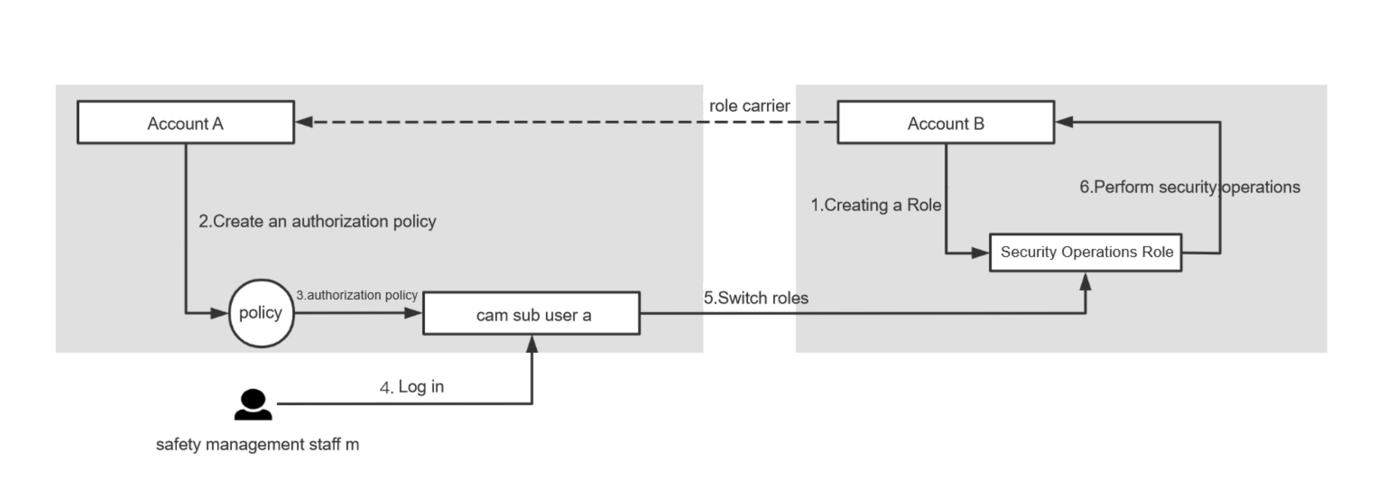
Role

Last updated：2023-08-31 18:46:48

Role Overview

A role is a virtual user in CAM that can be granted permission policies and possesses the corresponding permissions of the primary account. For more details, see Role Overview.

When creating a role, you can choose to use a Tencent Cloud primary account as the role carrier, create the role, and bind authorization policies to the role. The primary account acting as the carrier can create permission policies to grant the role-playing permissions to its CAM sub-accounts. Subsequently, CAM sub-accounts can switch roles to log in to the corresponding primary account console via the Tencent Cloud console and perform operations within the authorized scope. They can also initiate cross-account requests through the Cloud API.\n



Scenario

Suppose there are two primary accounts, Account A and Account B, within an enterprise. Employee M has a CAM sub-user 'a' under Account A and wishes to use this sub-account to simultaneously manage the security information under Account B. In this case, we can proceed with the following steps:

Instructions

1. Create a security operation role 'role' under Account B and designate the primary Account A as the role carrier. For detailed operations, please refer to Create Role.
2. Create a permission policy under Account A, which supports role-playing the security operation role 'role' through AssumeRole.
3. Grant the policy to CAM sub-user 'a'.\nFor detailed operations, please refer to Assigning Role-Playing Policy to Sub-Account.
4. Employee M logs in to CAM sub-user 'a'.
5. Employee M selects 'Switch Role' on the Tencent Cloud console and logs in to the Tencent Cloud console using the security role 'role'. For detailed operations, please refer to Logging in to Tencent Cloud Console Using a Role.
6. Perform security operations and maintenance related actions.
7. If Employee M needs to perform security operations on multiple primary accounts simultaneously, the above steps can be followed to grant Employee M the necessary security operation permissions for the corresponding primary accounts.

Collaborators

Last updated：2024-02-01 20:53:52

Collaborator Overview

The collaborator inherently possesses the identity of a primary account. Once added as a collaborator to the current primary account, it becomes one of the sub-accounts of the current primary account, assisting in the management of cloud resources under the primary account.

Scenario

Assume that an enterprise has multiple accounts on the cloud, such as Account A, Account B, Account C, etc., and it is desired that Account B and Account C have access permission to the resources under Account A.

Instructions

1. Account A logs into the Cloud Access Management Console, adds Account B and Account C as collaborators, and grants them permissions. For detailed operations, please refer to Create Collaborator and Collaborator Permission Settings.
2. Account B or Account C logs in to the Tencent Cloud Console as a collaborator. For detailed operations, see Sub-account Console Login - Collaborator Login.
3. If you intend to switch to access another account, you need to log out and log in again. For detailed operations, see Switching Collaborator Identity.

View the Tencent Cloud operation records of employees

Last updated：2024-02-01 20:55:38

Scenario

Once you have created a CAM sub-user for your employees and granted them permissions, they can log in to the Tencent Cloud Console using the CAM sub-user credentials, or use the CAM sub-user key to access and operate resources under your account via the cloud API. When a large number of employees need to log in to Tencent Cloud and access resources simultaneously, you may need to understand the following information:

- Which resources have been accessed by the employees?
- Have the employees encountered any issues during their operations?
- Which employee purchased a particular resource?
- How to view the modification records of resource configurations?
- How to track sensitive operations?
- Are the employees accessing Tencent Cloud within the environment you have specified?

At this point, you can use CloudAudit to view and track the operation records of your employees. CloudAudit supports online viewing of Tencent Cloud console and cloud API operation records within the past 90 days.

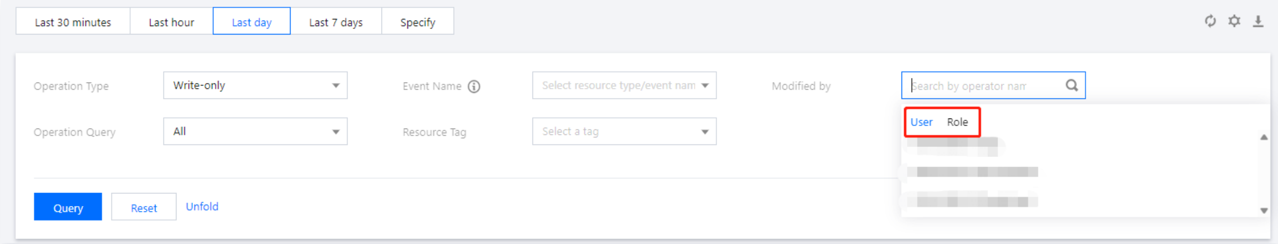
Preparations

1. You have created a sub-user. For more information, see Create a Sub-User.
2. You have logged in to the CloudAudit Console and navigated to the Operation Record page.

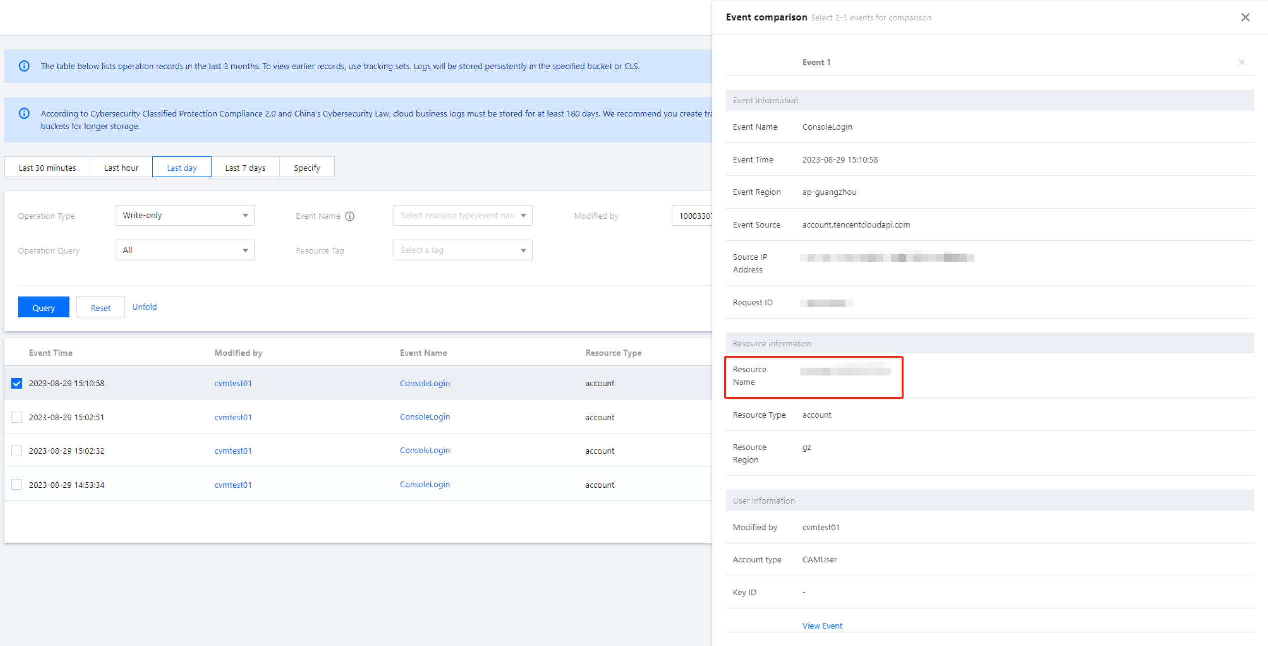
Instructions

Viewing Event Details in Operation Record

- You can filter by "Operator" to search according to the CAM sub-user/role, and view the operation records of specific employees.



- In the detailed log summary, identify the actual operating account ID and name through the user field, and check the operation source through the source IP address.



ⓘ The table below lists operation records in the last 3 months. To view earlier records, use tracking sets. Logs will be stored persistently in the specified bucket or CLS.

ⓘ According to Cybersecurity Classified Protection Compliance 2.0 and China's Cybersecurity Law, cloud business logs must be stored for at least 180 days. We recommend you create tra buckets for longer storage.

Operation Type: Write-only
Event Name ⓘ: Select resource type/event nam
Modified by: 1000330
Operation Query: All
Resource Tag: Select a tag

	Event Time	Modified by	Event Name	Resource Type
☑	2023-08-29 15:10:58	cvmtest01	ConsoleLogin	account
□	2023-08-29 15:02:51	cvmtest01	ConsoleLogin	account
□	2023-08-29 15:02:32	cvmtest01	ConsoleLogin	account
□	2023-08-29 14:53:34	cvmtest01	ConsoleLogin	account

Event comparison Select 2-5 events for comparison

Event 1

Event information

Event Name	ConsoleLogin
Event Time	2023-08-29 15:10:58
Event Region	ap-guangzhou
Event Source	account.tencentcloudapi.com
Source IP Address	[redacted]
Request ID	[redacted]

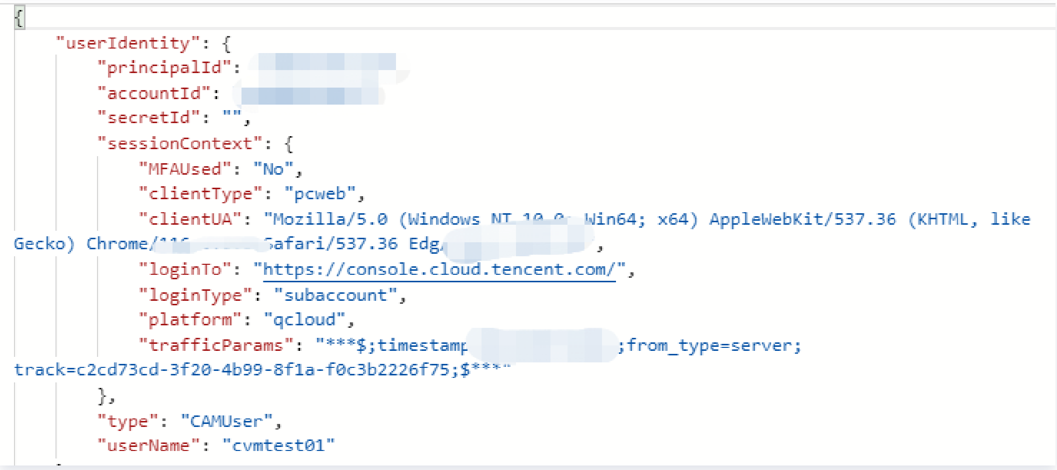
Resource information

Resource Name	[redacted]
Resource Type	account
Resource Region	gz

User Information

Modified by	cvmtest01
Account type	CAMUser
Key ID	-

- In the detailed log information, you can identify the actual operating account ID through the principalId.



```
{
    "userIdentity": {
        "principalId": [redacted]
        "accountId": [redacted]
        "secretId": "",
        "sessionContext": {
            "MFAUsed": "No",
            "clientType": "pcweb",
            "clientUA": "Mozilla/5.0 (Windows NT [redacted] Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/[redacted]afari/537.36 Edg[redacted] ,
            "loginTo": "https://console.cloud.tencent.com/",
            "loginType": "subaccount",
            "platform": "qcloud",
            "trafficParams": "***$;timestamp[redacted];from_type=server;
track=c2cd73cd-3f20-4b99-8f1a-f0c3b2226f75;$***"
        },
        "type": "CAMUser",
        "userName": "cvmtest01"
```

For detailed operations, see: View Operation Record Event Details.

Shipping Log with Tracking Set

If you need to view a longer history of employee operation records, you can utilize the tracking set feature of CloudAudit to deliver logs to a Cloud Object Storage (COS) bucket or CLS.

When shipping to CLS, you can select specific operations for a designated product (such as sensitive operations) and configure alerting policies within CLS.

For detailed operations, see: Using Tracking Sets to Deliver Logs.

Setting up cross-account log delivery for group accounts

If you have multiple primary accounts on Tencent Cloud, you can use CloudAudit tracking sets to centrally track and view operation records. For detailed operations, see: Setting up cross-account log delivery for group accounts.

Utilizing API for Enterprise Multi-Account Permissions Management

Last updated：2024-02-01 20:57:12

Scenario

Many enterprise clients build internal IT systems to manage the process of employee sub-account applications. When there are multiple accounts within the enterprise, combining group accounts with Cloud Access Management (CAM) can significantly enhance management efficiency and security.

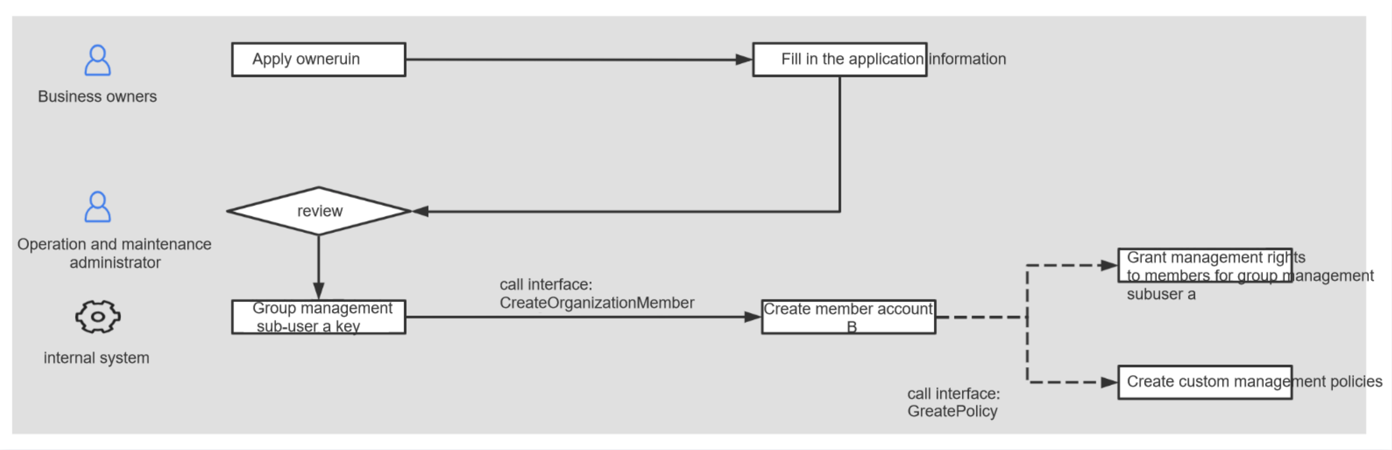
Suppose that:

- The company already has Account A, which has been enabled as the admin account for the Tencent Cloud Organization service.
- Under Account A, there is a CAM sub-user 'a' with full administrative permissions.
- Within the company, there is a game business manager, Xiao Wang, who wants to apply for a new root account to run a newly released game. He also wants to apply for a sub-user with development permissions for a developer, Xiao Li, under this root account for daily access to Tencent Cloud.

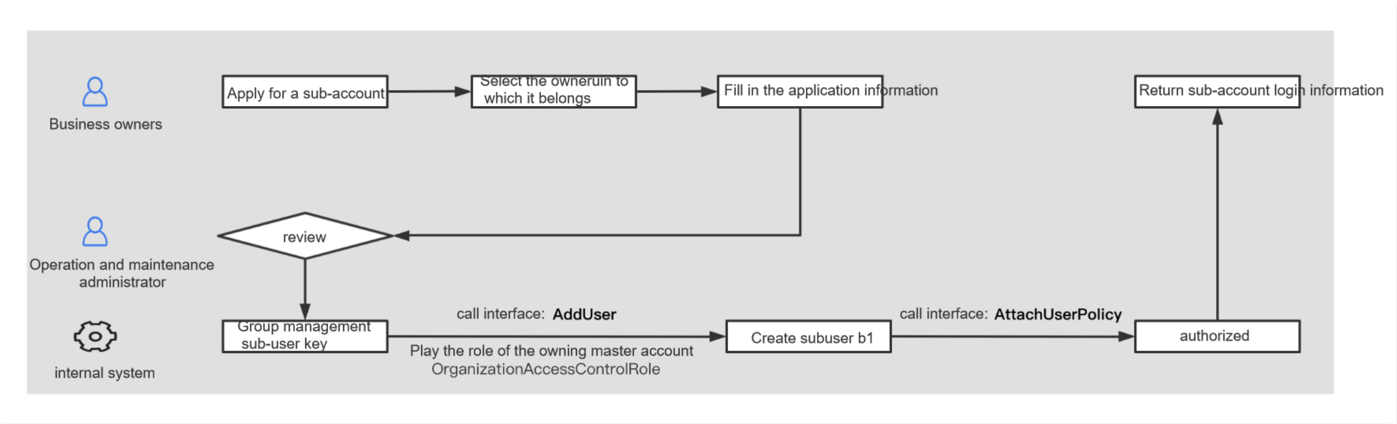
Process Description

The entire process of creating the main account and applying for and authorizing sub-accounts is completed using the key of CAM sub-user 'a'.

Procedure 1: Apply for a primary account for the new game


Business owners
Apply owneruin
Fill in the application information
Operation and maintenance administrator
review
internal system
Group management sub-user a key
call interface: CreateOrganizationMember
Create member account B
Grant management rights to members for group management subuser a
call interface: GreatePolicy
Create custom management policies

Procedure 2: Create a CAM sub-account for developer Li and grant permissions


Business owners
Apply for a sub-account
Select the ownerUin to which it belongs
Fill in the application information
Return sub-account login information
Operation and maintenance administrator
review
internal system
Group management sub-user key
call interface: AddUser
Play the role of the owning master account OrganizationAccessControlRole
Create subuser b1
call interface: AttachUserPolicy
authorized

Instructions

Utilize the admin sub-user 'a' to create an account for the new business.

1. Invoke the CreateOrganizationMember API of the Tencent Cloud Organization service to create a new root account.

> **Note**
> - The created main account uses the real-name information of the group management account and automatically completes the enterprise identity verification.
> - The created primary account, the admin account, will automatically have management permissions.
> - Additionally, financial management permissions can be assigned to newly created accounts. Currently, five types of permissions are supported: viewing member account bills, viewing member account consumption, allocating funds to member accounts, applying for invoices on behalf of member accounts, and consolidated billing.
> - You can also set the payment method for member accounts: Self-paying + Inherit discounts, or Pay-on-behalf.
> - For information on managing member finances, please refer to Viewing Financial Permissions.

2. The group account management API grants sub-user 'a' the permission to manage newly created primary accounts.
   2.1 Under the management account A, create a policy with admin management permissions for the new account: CreateOrganizationMemberPolicy
   2.2 Grant the newly created policy to the management sub-account 'a': BindOrganizationMemberAuthAccount
3. Invoke the CreatePolicy API of the Cloud Access Management service to create the required custom authorization policy under the created account (execute as needed).

> **Note**
> If the preset policies can meet the authorization requirements, this step can be disregarded.

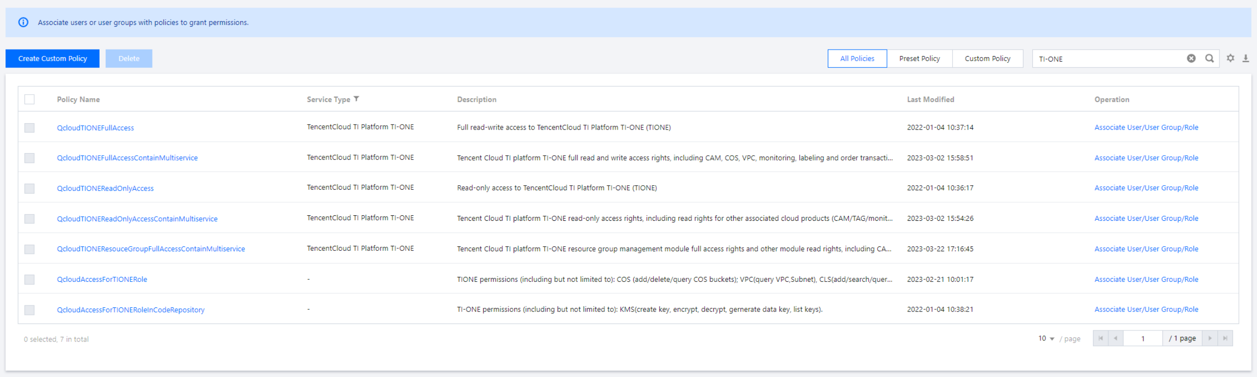
At this point, the process of creating an account for the new game is complete. If you need to activate multiple accounts simultaneously, you can repeat the above process.

The admin sub-user 'a' is used to create CAM sub-accounts for employees.

1. Invoke the AddUser API of the Access Management service to create a sub-user under the newly created Tencent Cloud account.

> **Note**
> The creation of a sub-user requires an administrator identity and assumes the role of the created member, OrganizationAccessControlRole. For API role invocation, refer to the Using Roles document.

2. Obtain the Policy ID that needs to be associated with the policy.
   2.1 In the **Policies** page of the Cloud Access Management Console, search for the policy that needs to be bound (for example, the full read/write policy of TI-ONE).



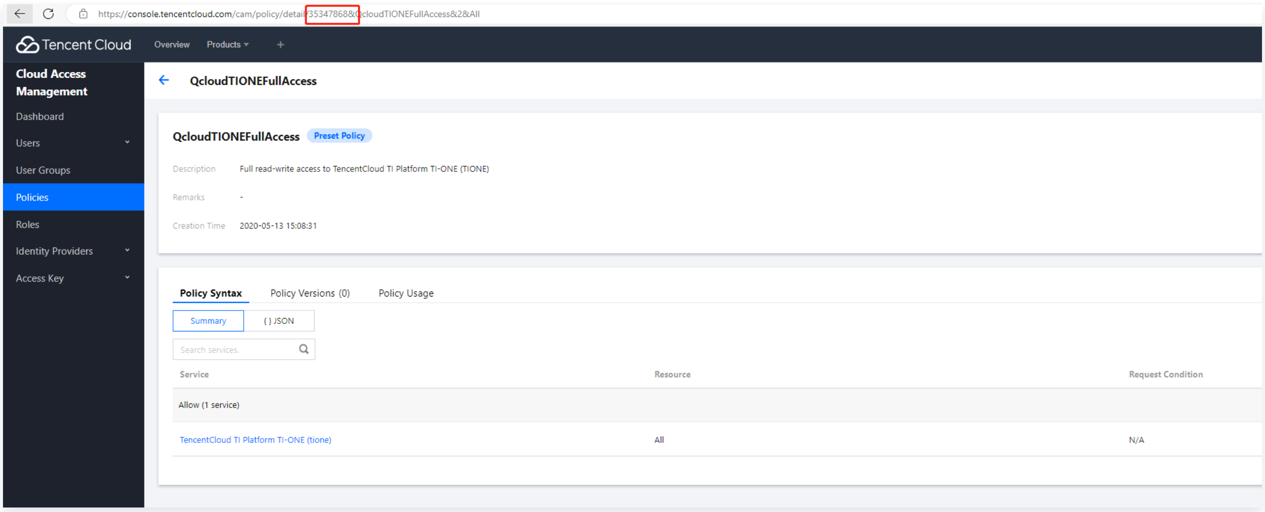
Associate users or user groups with policies to grant permissions.

Policy Name	Service Type	Description	Last Modified	Operation
QcloudTIONEFullAccess	TencentCloud TI Platform TI-ONE	Full read-write access to TencentCloud TI Platform TI-ONE (TIONE)	2022-01-04 10:37:14	Associate User/User Group/Role
QcloudTIONEFullAccessContainMultiservice	TencentCloud TI Platform TI-ONE	Tencent Cloud TI platform TI-ONE full read and write access rights, including CAM, COS, VPC, monitoring, labeling and order transacti...	2023-03-02 15:58:51	Associate User/User Group/Role
QcloudTIONEReadOnlyAccess	TencentCloud TI Platform TI-ONE	Read-only access to TencentCloud TI Platform TI-ONE (TIONE)	2022-01-04 10:36:17	Associate User/User Group/Role
QcloudTIONEReadOnlyAccessContainMultiservice	TencentCloud TI Platform TI-ONE	Tencent Cloud TI platform TI-ONE read-only access rights, including read rights for other associated cloud products (CAM/TAG/monit...	2023-03-02 15:54:26	Associate User/User Group/Role
QcloudTIONEResouceGroupFullAccessContainMultiservice	TencentCloud TI Platform TI-ONE	Tencent Cloud TI platform TI-ONE resource group management module full access rights and other module read rights, including CA...	2023-03-22 17:16:45	Associate User/User Group/Role
QcloudAccessForTIONERole	-	TIONE permissions (including but not limited to): COS (add/delete/query COS buckets); VPC(query VPC,Subnet), CLS(add/search/quer...	2023-02-21 10:01:17	Associate User/User Group/Role
QcloudAccessForTIONERoleInCodeRepository	-	TI-ONE permissions (including but not limited to): KMS(create key, encrypt, decrypt, gernerate data key, list keys).	2022-01-04 10:38:21	Associate User/User Group/Role

0 selected, 7 in total

10 / page 1 / 1 page

   2.2 Click on the policy name to enter the policy details page. The policy ID can be found in the following location in the browser's address bar.



https://console.tencentcloud.com/cam/policy/detail/35347868&QcloudTIONEFullAccess&2&All

QcloudTIONEFullAccess

QcloudTIONEFullAccess Preset Policy

Description: Full read-write access to TencentCloud TI Platform TI-ONE (TIONE)

Remarks: -

Creation Time: 2020-05-13 15:08:31

Service	Resource	Request Condition
Allow (1 service)		
TencentCloud TI Platform TI-ONE (tione)	All	N/A

3. Invoke the Access Management product's AttachUserPolicy API to authorize the created sub-user.

Utilize ABAC to regulate employee resource access permissions

Overview of ABAC

Last updated：2024-02-01 20:59:21

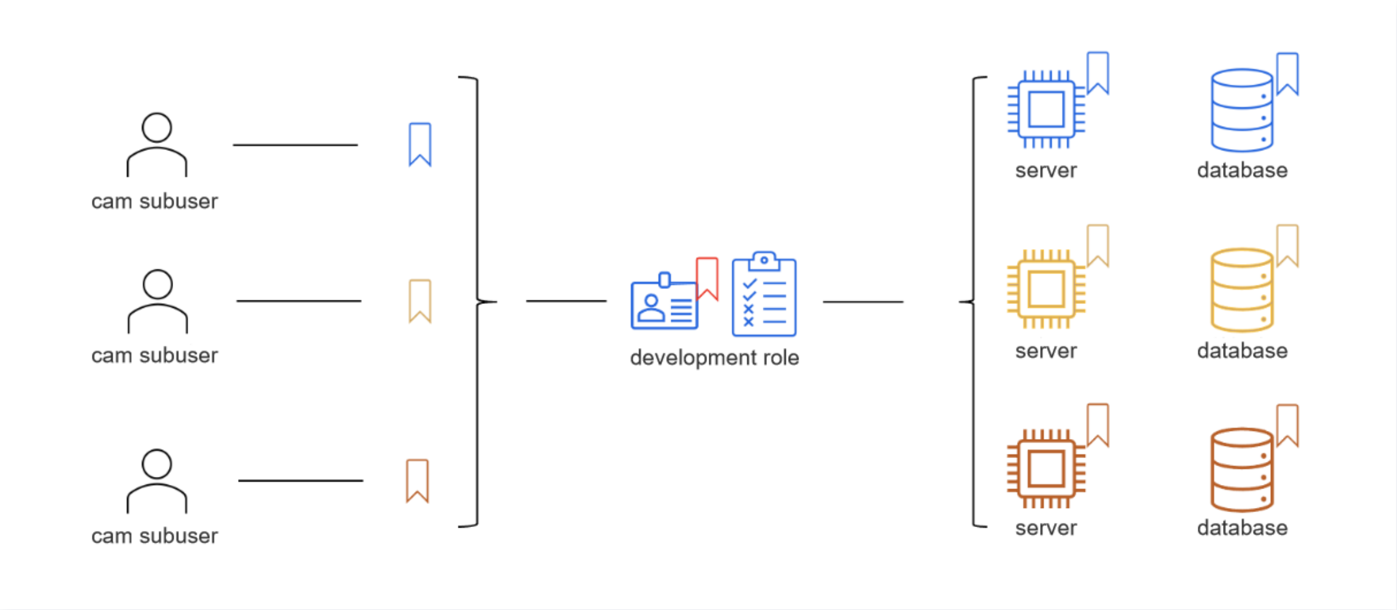
Introduction to ABAC

What is ABAC?

ABAC (Attribute-Based Access Control) is an attribute-based access control policy that uses attributes to define permissions. In Tencent Cloud, tags are used to represent these attributes.
When creating resources in Tencent Cloud, you can attach tags to the resources to mark them (see Products that support tags). When granting permissions to a role, you can create a single ABAC policy and design it to allow operations when the tags of the role request match the resource tags. ABAC is very useful in environments where resources change frequently, and it helps you improve management efficiency when policy management becomes cumbersome.

Assume that there are three projects, GroupA, GroupB, and GroupC, each with developers a, b, and c respectively. You can manage employee resource access permissions through the following steps:

1. Create three CAM sub-users for the three employees, each with tag keys of GroupA, GroupB, and GroupC respectively, and tag values of dev. Grant assumeRole permissions to these three sub-users.
2. Create a development role, with the corresponding role tag value set to dev.
3. Use a single policy to allow access to resources under the three projects, and attach the policy to the created roles.
4. Employees access resources by assuming roles through CAM sub-users. Access is permitted when the tag key of the employee matches the tag value of the resource.



Comparison between ABAC and Traditional Authorization Methods

In CAM, you control permissions by creating different policies for employees in different job positions, and then you can attach these policies to CAM roles. According to Best Practices, when granting employees the minimum necessary permissions, you typically do so by specifying the specific resources that can be accessed in the policy. The downside of this approach is that when an employee needs to add access to new resources, the policy must be updated to allow access to these resources.
Assume that there are three projects, GroupA, GroupB, and GroupC, each with different resources. The comparison of the two authorization methods is as follows:

Authorization	ABAC Authorization	Traditional Authorization

Method		
Authorization for the same position in the three projects	1. Three Sub-Users 2. One Role 3. Two policies (three sub-users share one role-switching policy, and each role has one permission management policy)	1. Three Sub-Users 2. Three roles 3. Six policies (each sub-user has one role-switching policy, and each role has one permission management policy)
Adding/Reducing Resources to a Single Project	No adjustments to the authorization policy are required.	Adjust the permission management policy corresponding to the role.
Adding a new project	Simply create a new sub-user.	It is necessary to create new sub-users, roles, and the two associated policies.

Advantages of ABAC Authorization

Utilizing ABAC to manage resource access permissions offers the following advantages:

Automatic Expansion of Resource Permissions

Permissions can now automatically expand with resource changes, eliminating the need for administrators to update existing policies to allow access to new resources.

For example, assume that you attach the access-project tag to the ABAC policy. Developers use the access-project = GroupA tag to access resources. When employees in the GroupA project need additional CVM cloud server resources, developers can create new CVM instances using the access-project = GroupA tag. Once created, any authorized employee in the GroupA project can start and stop these instances, as the tags of the roles corresponding to the employees in the GroupA project match the tags of the resources.

Reduce the number of policies

It reduces the number of policies required. There is no longer a need to create different policies for employees in the same position across different projects. As a result, the number of policies created is reduced, making management more straightforward.

Facilitate subsequent policy expansion

If there are new projects, you can quickly expand based on existing policies.

For instance, if you are already managing resource access permissions for projects GroupA and GroupB, you can quickly support the newly added project GroupD. The CAM administrator can create a new sub-user corresponding to GroupD, assign the corresponding tags to GroupD, and then grant the sub-user the policy to switch roles. At this point, any employee with the authority to assume this role can access resources tagged with access-project = GroupD.

Achieve Fine-Grained Access Control

When creating policies, the best practice is to grant the least permission. Using traditional authorization methods, you must write a policy that only allows access to specific resources. However, with ABAC, you can permit operations on all resources, but access to those permissions is only allowed when the resource tags match the principal's tags.

Scenarios

Last updated：2024-02-01 21:01:04

Scenario

In practical use of Tencent Cloud, we can utilize tags to define permissions through the ABAC authorization policy. Tags can be bound to CAM sub-users, roles, and specific cloud resources. Subsequently, permission policies can be defined, which use tag condition keys to grant permissions based on the tags of the requesting identity. When you control access to Tencent Cloud resources using tags, changes to teams and resources can be implemented with fewer modifications to the authorization policy, making operations more flexible.

This section will provide a detailed explanation on how to create a CAM role with tags for employees in CAM, as well as a permission policy that allows access to resources matching the role's attributes. When an employee makes a request to Tencent Cloud through this role, permissions will be granted based on whether the role's tags match the resource tags, thus allowing employees to view or operate only the resources necessary for their work.

Sample Code

Suppose in gaming company A, there are two projects: webpage and app. Employee m is a developer for the webpage project, and employee n is a developer for the app project. When creating the authorization policy, it is necessary to ensure that employees within different teams can access the resources required for their work, while also considering scalability for future company growth.

You can create authorization policies for products that support ABAC strategies by using resource tags and CAM role tags. When your employees wish to access Tencent Cloud through federated identities, their attributes will be applied to the role tags in Tencent Cloud. Subsequently, you can use ABAC to allow or deny access based on these attributes.

> **Note**
> - Refer to Products Supporting Tags to understand which products support tag-based authorization.
> - Refer to Overview of Effective Conditions to understand which tag condition keys are supported in the authorization policy.

Based on the aforementioned projects and teams, we define the following tags:

- game-project = web (corresponding to the web project)
- game-project = app (corresponding to the app project)
- web = dev (corresponding to web project developers)
- app = dev (corresponding to the app developer)

How to Implement

1. Employees log in using IAM user credentials and then assume the CAM role of their respective team and project.
2. The same policy will be attached to roles of the same position, with permissions or denials implemented based on tags.

Verification Scenario

Assume there are two cloud servers, ins-78qewdr8 (tagged with game-project:app) and ins-7txjj4a6 (tagged with game-project:web), which belong to the app and webpage projects respectively.

- Validation Point 1: After employees from different projects log in using different CAM sub-users, how can we ensure that each employee can only access the cloud servers under their respective projects?
- Verification Point 2: Suppose there is a change in employee roles, and employee n also needs access to the webpage project. How can permissions be adjusted quickly?
- Validation Point 3: Suppose the company adds a new H5 class project, how can we quickly grant employees permissions for the new project?

Instructions

Step 1: Create a Test CAM Sub-user

1. Create a custom policy named `access-assume-role`. The policy content is "Allow the assumption of ABAC roles when the tags of the assumed identity match the role tags."

> **Note**
> For detailed instructions on creating a CAM policy, please refer to Creating a Role.

```
    {
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "sts:AssumeRole"
      ],
      "resource": "*",
      "condition": {
        "for_any_value:string_equal": {
          "qcs:resource_tag": [
            "game&${qcs:principal_tag_value}"
  ]
 }
 }
   },
    {
      "effect": "allow",
      "action": [
        "cam:ListUserTags",
        "cam:ListLoginRoles"
      ],
      "resource": [
        "*"
  ]
 }
  ]
 }
```

2. Create CAM sub-users m-developer and n-sysmanager, bind the access-assume-role authorization policy to these sub-users, and attach the following tags to them.

> **Note**
> For detailed instructions on creating a CAM sub-user, please refer to Create Sub-User.

Sub-user Name	Associated Tags
m-developer	web=dev
n-developer	app=dev

Step 2: Create an ABAC policy

1. Create a custom policy named 'access-resource-project' (using the cvm product as an example). The policy content is as follows:

```
    {
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": "cvm:*",
      "resource": "*",
      "condition": {
        "for_any_value:string_equal": {
          "qcs:request_tag": [
            "game-project&${qcs:principal_tag_key}"
  ]
  }
  }
     },
     {
      "effect": "allow",
      "action": "cvm:*",
      "resource": "*",
      "condition": {
        "for_any_value:string_equal": {
          "qcs:resource_tag": [
            "game-project&${qcs:principal_tag_key}"
  ]
  }
  }
     },
     {
      "effect": "allow",
      "action": [
        "vpc:DescribeVpcEx",
        "vpc:DescribeSubnetEx",
        "vpc:DescribeNetworkInterfaces",
        "cvm:DescribeDiskSecurityConfigurations",
        "cvm:DescribeCbsStorages",
        "tag:DescribeTagKeys",
        "tag:DescribeTagValues"
      ],
      "resource": [
        "*"
  ]
  }

  ]
  }
```

2. Create the role 'access-developer-role', associate it with the aforementioned policy, and bind the following tags.

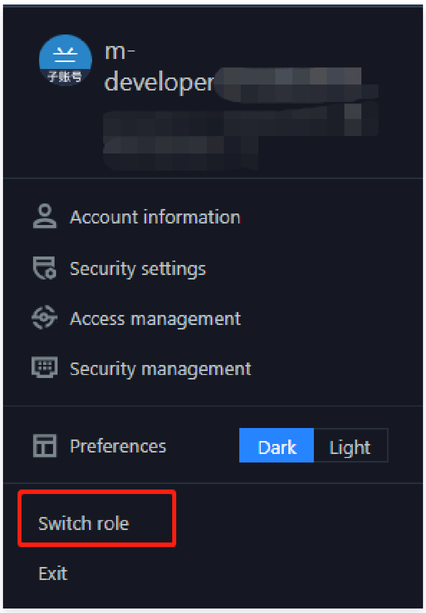
> **Note**
> For detailed instructions on creating a CAM policy, please refer to Creating a Role.

CAM Role Name	Associated Tags
access-developer-role	game=dev

Step 3: Scenario Verification

Validation Point 1: After logging in with different sub-users, they can only access the CVMs under their respective projects.

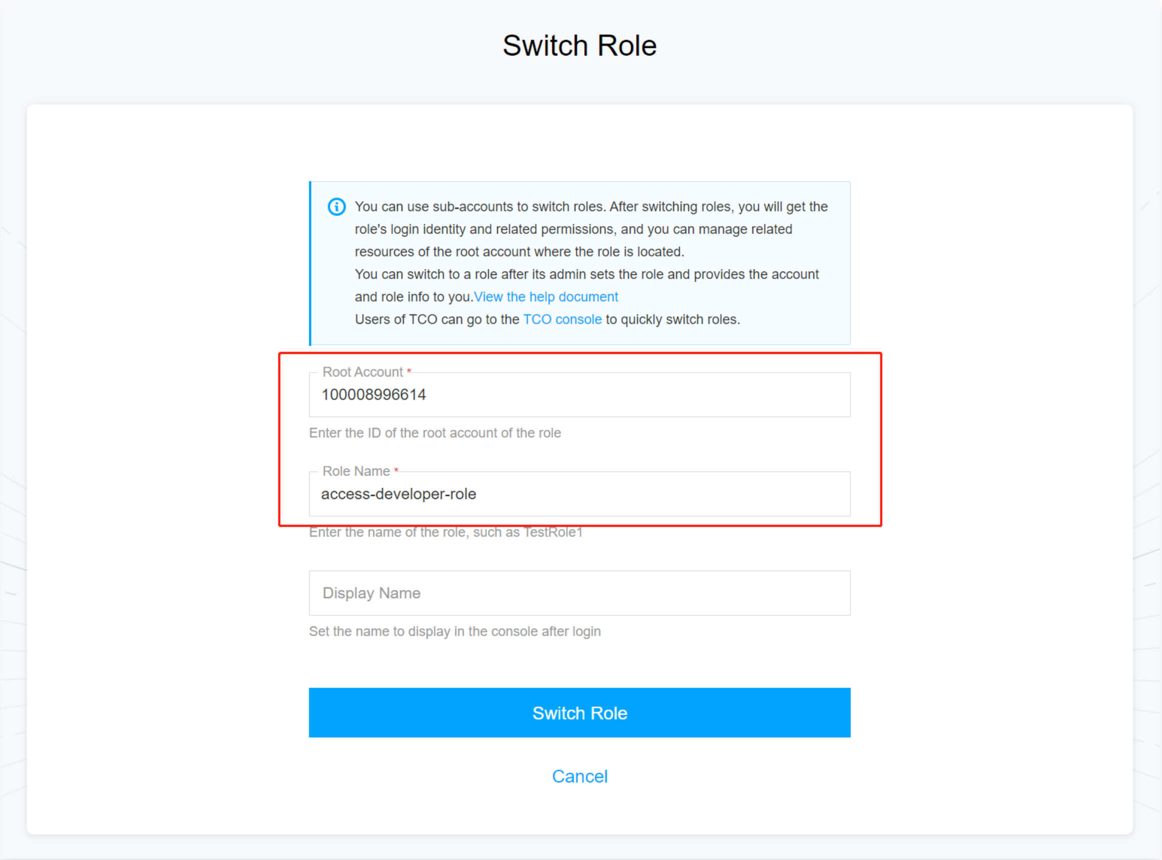
1. Log in to the Tencent Cloud console as the sub-user m-developer. In the upper right corner of the console, click **Switch Role** under the account.



m-developer [redacted]

[redacted]

2. On the Switch Role page, select 'web' for the application (which is the tag value for sub-user m-developer), choose 'access-developer-role' for the role, and then click **Switch Role**.



Switch Role

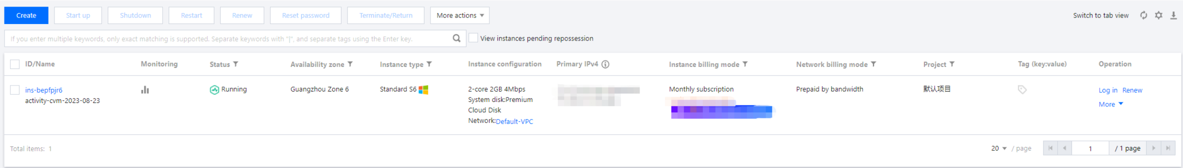
You can use sub-accounts to switch roles. After switching roles, you will get the role's login identity and related permissions, and you can manage related resources of the root account where the role is located.
You can switch to a role after its admin sets the role and provides the account and role info to you. View the help document
Users of TCO can go to the TCO console to quickly switch roles.

Root Account *: 100008996614
Enter the ID of the root account of the role

Role Name *: access-developer-role
Enter the name of the role, such as TestRole1

Display Name
Set the name to display in the console after login

3. Log in to the Tencent Cloud console as a role, and navigate to the CVM **Instance** page.
In the CVM product console, if you can only view ins-bepfpjr6 (tagged with game-project:web), then it meets the expectations.



If you enter multiple keywords, only exact matching is supported. Separate keywords with "|", and separate tags using the Enter key.

□ View instances pending repossession

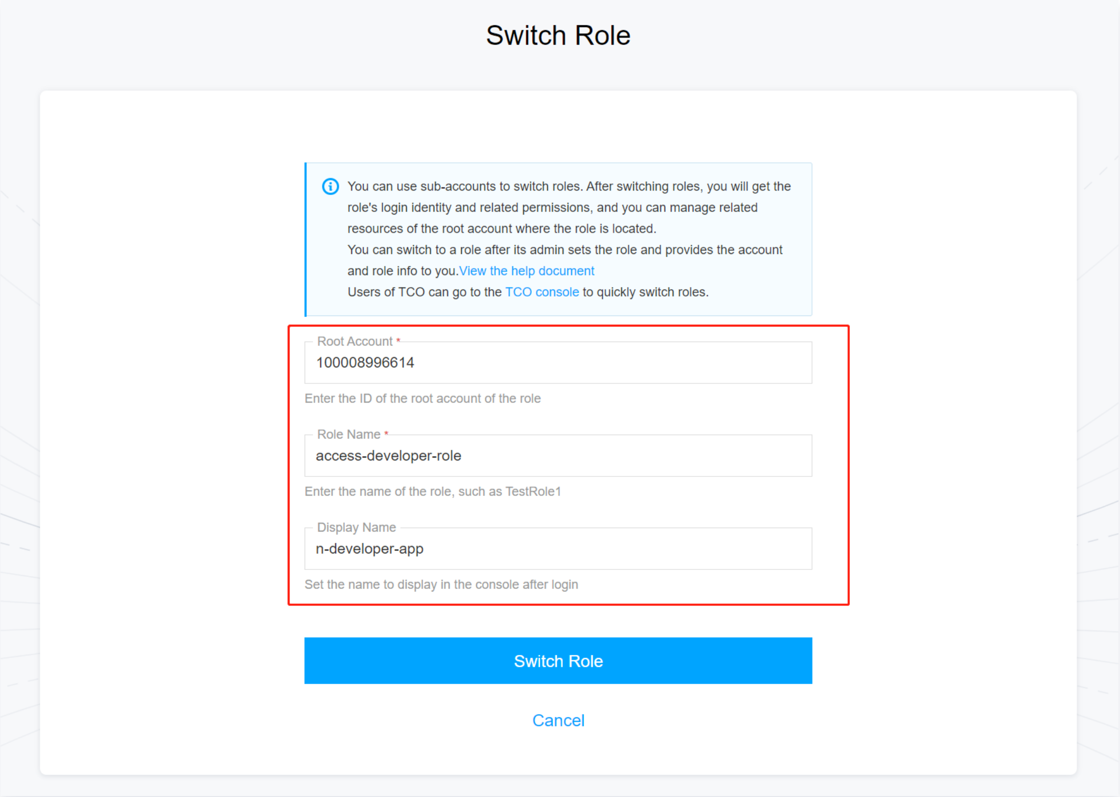
□ ID/Name	Monitoring	Status	Availability zone	Instance type	Instance configuration	Primary IPv4	Instance billing mode	Network billing mode	Project	Tag (key:value)	Operation
□ ins-bepfpjr6 activity-cvm-2023-08-23		Running	Guangzhou Zone 6	Standard S6	2-core 2GB 4Mbps System disk:Premium Cloud Disk Network:Default-VPC	[redacted]	Monthly subscription [redacted]	Prepaid by bandwidth	默认项目		Log in Renew More

Total items: 1

20 / page 1 / 1 page

4. Switch identity and log in to the Tencent Cloud Console as the sub-user n-developer. After logging in, switch roles, select app

for the application, choose access-developer-role for the role, and set the display name as n-developer-app. Then click **Switch Role**.



Switch Role

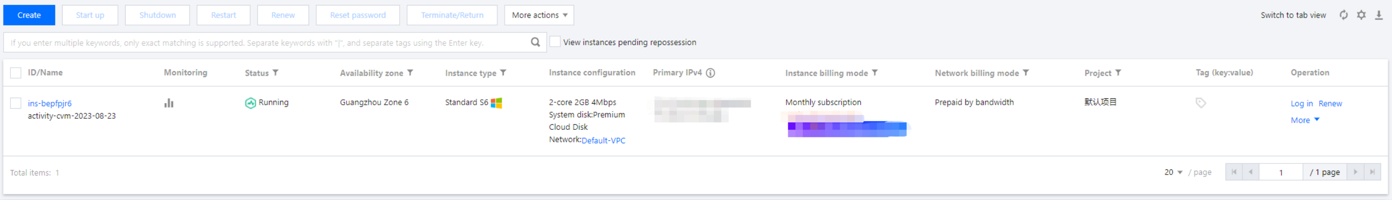
You can use sub-accounts to switch roles. After switching roles, you will get the role's login identity and related permissions, and you can manage related resources of the root account where the role is located.
You can switch to a role after its admin sets the role and provides the account and role info to you.View the help document
Users of TCO can go to the TCO console to quickly switch roles.

Root Account *
100008996614
Enter the ID of the root account of the role

Role Name *
access-developer-role
Enter the name of the role, such as TestRole1

Display Name
n-developer-app
Set the name to display in the console after login

5. Enter the Tencent Cloud console as a role, and navigate to the CVM Instance page.
   In the CVM product console, if you can only view the cloud server ins-bepfpjr6 (tagged game-project:app), then it meets the expectations.



If you enter multiple keywords, only exact matching is supported. Separate keywords with "|", and separate tags using the Enter key.

□ View instances pending repossession

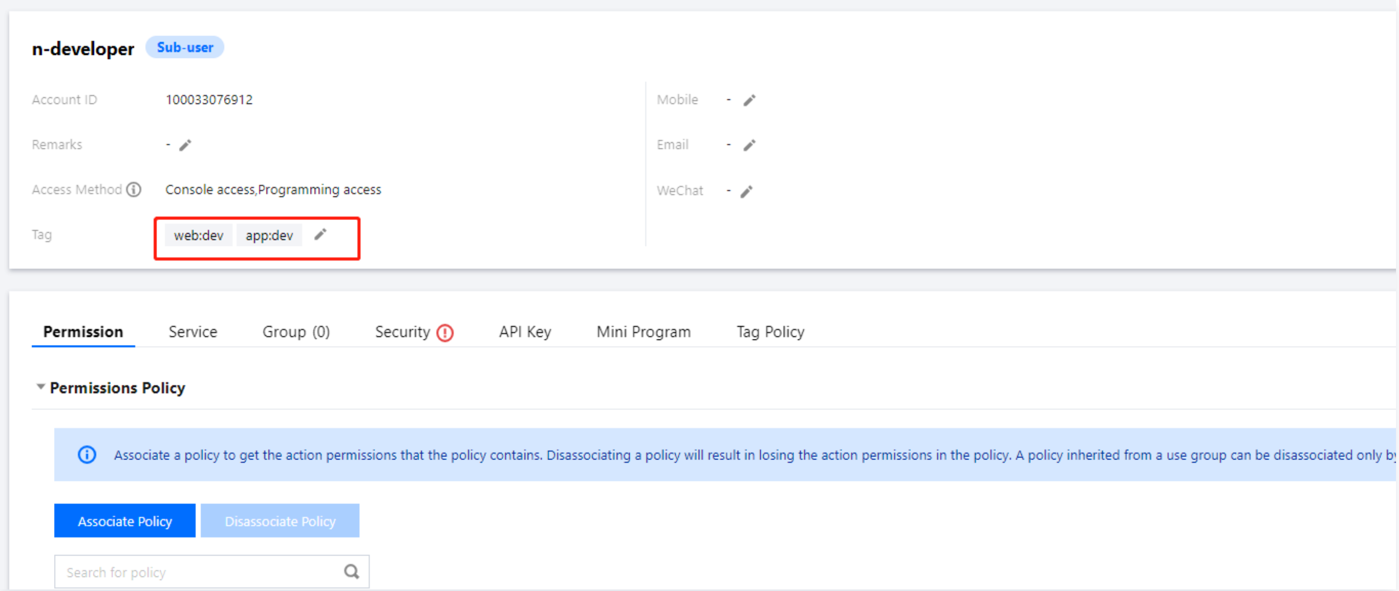
ID/Name	Monitoring	Status	Availability zone	Instance type	Instance configuration	Primary IPv4	Instance billing mode	Network billing mode	Project	Tag (key:value)	Operation
ins-bepfpjr6 activity-cvm-2023-08-23		Running	Guangzhou Zone 6	Standard S6	2-core 2GB 4Mbps System disk:Premium Cloud Disk Network:Default-VPC	[redacted]	Monthly subscription [redacted]	Prepaid by bandwidth	默认项目		Log in Renew More

Total items: 1

20 / page 1 / 1 page

Verification Point 2: Suppose there is a job change and employee n also needs access to the webpage project. How should this be set up?

In the current scenario, all we need to do is add the tag app:web to the CAM sub-user n-developer corresponding to employee n in the user details of the Cloud Access Management Console.



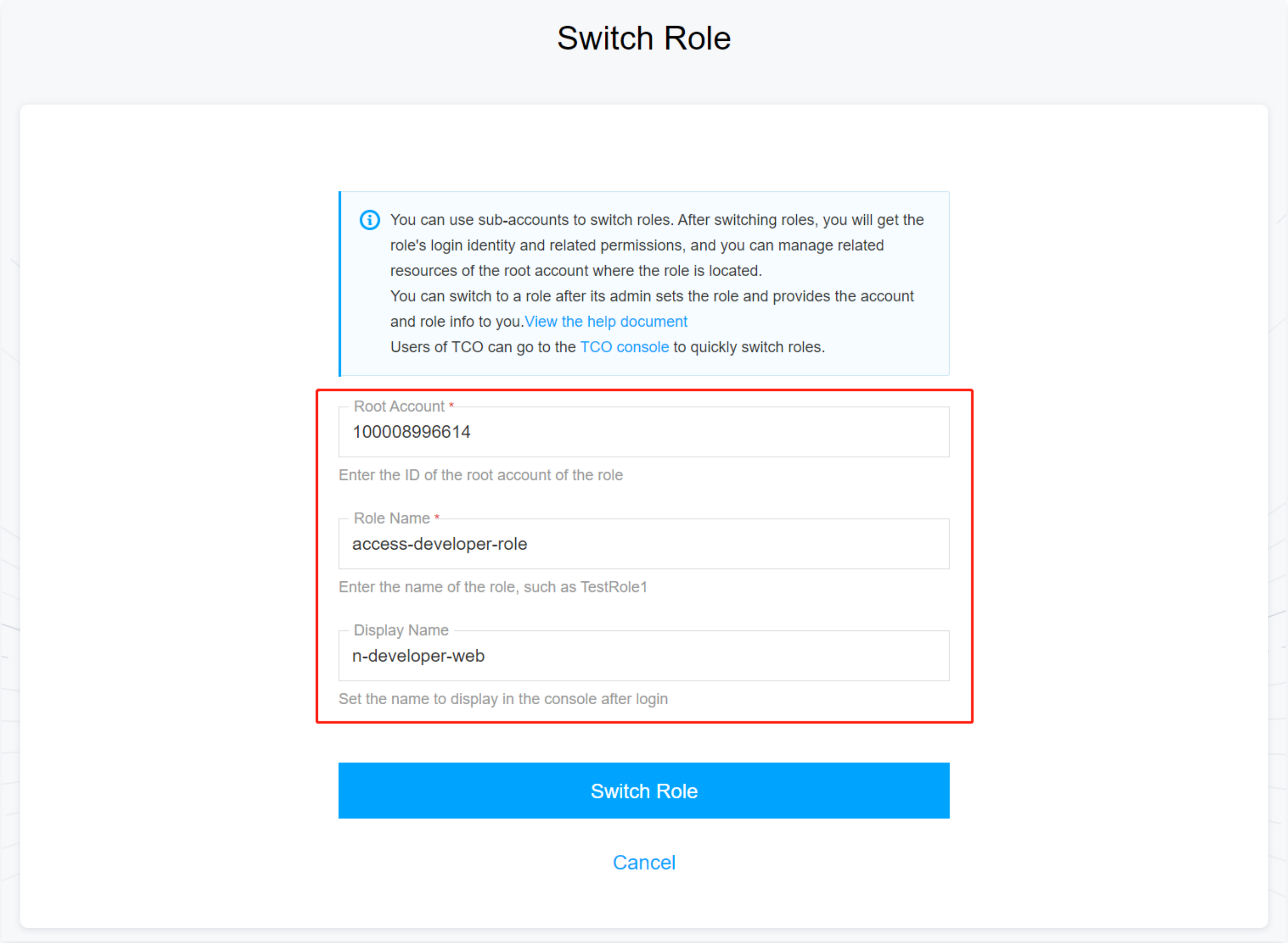
n-developer Sub-user

Account ID	100033076912	Mobile	-
Remarks	-	Email	-
Access Method	Console access,Programming access	WeChat	-
Tag	web:dev app:dev		

Permissions Policy

Associate a policy to get the action permissions that the policy contains. Disassociating a policy will result in losing the action permissions in the policy. A policy inherited from a use group can be disassociated only by

1. Log in to the Tencent Cloud console as the sub-user n-developer. In the upper right corner of the console, click **Switch Role** under the account.
2. On the Switch Role page, select 'web' for the application, 'access-developer-role' for the role, and 'n-developer-web' for the alias. Then click **Switch Role**.



Switch Role

You can use sub-accounts to switch roles. After switching roles, you will get the role's login identity and related permissions, and you can manage related resources of the root account where the role is located.
You can switch to a role after its admin sets the role and provides the account and role info to you.View the help document
Users of TCO can go to the TCO console to quickly switch roles.

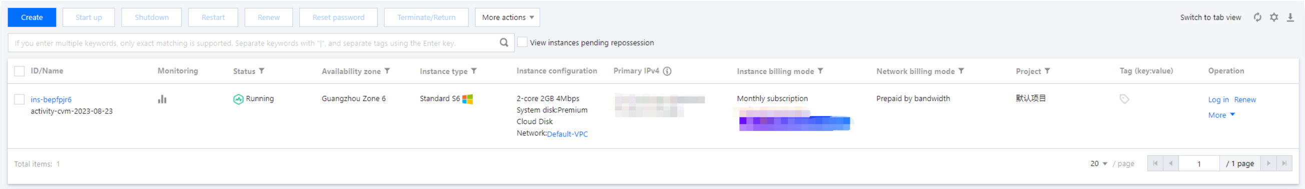
Root Account *: 100008996614
Enter the ID of the root account of the role

Role Name *: access-developer-role
Enter the name of the role, such as TestRole1

Display Name: n-developer-web
Set the name to display in the console after login

3. Log in to the Tencent Cloud console as a role and navigate to the CVM Instance page.
In the CVM product console, if you can only view the cloud server ins-7txjj4a6 (tagged game-project:web), then it meets the

expectations.


Create
Start up
Shutdown
Restart
Renew
Reset password
Terminate/Return
More actions
Switch to tab view
If you enter multiple keywords, only exact matching is supported. Separate keywords with "|", and separate tags using the Enter key.
View instances pending repossession

ID/Name	Monitoring	Status	Availability zone	Instance type	Instance configuration	Primary IPv4	Instance billing mode	Network billing mode	Project	Tag (key:value)	Operation
ins-bepfpjr6 activity-cvm-2023-08-23		Running	Guangzhou Zone 6	Standard S6	2-core 2GB 4Mbps System disk:Premium Cloud Disk Network:Default-VPC	[redacted]	Monthly subscription [redacted]	Prepaid by bandwidth	默认项目		Log in Renew More

Total items: 1

20 / page 1 / 1 page

Validation Point 3: Suppose the company adds a new H5 class project, how should the permission policy be adjusted to accommodate this?

After the company adds a new H5 project, if we need to increase the development permissions for the H5 project, there is no need to change the policy itself. We only need to:

1. Create a new sub-user for the colleagues developing the HTML5 project.
2. Bind the tags corresponding to the H5 project to the sub-user and associate it with the access-assume-role policy.

When authorizing by tag, only matching the tag key is supported

Last updated：2024-02-01 21:02:12

This document outlines how to grant your sub-account permission to access all resources under a specific tag, as well as how to grant the sub-account the authority to bind only to a specific tag key.

Grant permissions to access all resources under a specific tag key (resource_tag)

Scenario

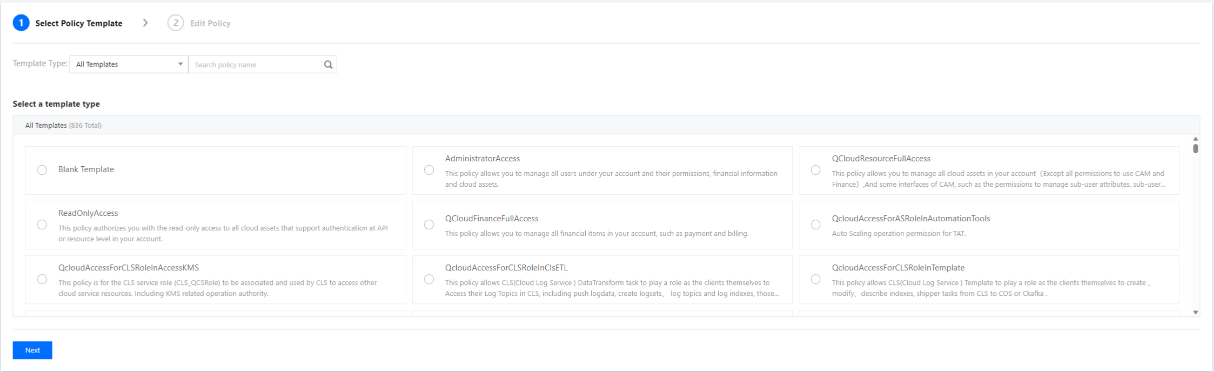
If your company has purchased a variety of Tencent Cloud resources, all managed through tag grouping, you may wish to grant access to all resources associated with a specific tag key (resource_tag).

Suppose that:

- There is a sub-account, DevA, under the enterprise account CompanyExample.
- The enterprise account, CompanyExample, has a tag key named test1.
- The enterprise account, CompanyExample, intends to grant the sub-account, DevA, access to all resources under the tag key test1.

Instructions

1. Log in to the Cloud Access Management Console as the enterprise account CompanyExample.
2. On the **Policies** page, click **Create Custom Policy** > **Create by Policy Syntax**.
3. Under the module type selection, choose the blank template and click **Next** to proceed to the policy editing page.



Template Type: All Templates
Search policy name

Select a template type

All Templates (836 Total)

○ Blank Template

○ AdministratorAccess
This policy allows you to manage all users under your account and their permissions, financial information and cloud assets.

○ QCloudResourceFullAccess
This policy allows you to manage all cloud assets in your account（Except all permissions to use CAM and Finance）,And some interfaces of CAM, such as the permissions to manage sub-user attributes, sub-user...

○ ReadOnlyAccess
This policy authorizes you with the read-only access to all cloud assets that support authentication at API or resource level in your account.

○ QCloudFinanceFullAccess
This policy allows you to manage all financial items in your account, such as payment and billing.

○ QcloudAccessForASRoleInAutomationTools
Auto Scaling operation permission for TAT.

○ QcloudAccessForCLSRoleInAccessKMS
This policy is for the CLS service role (CLS_QCSRole) to be associated and used by CLS to access other cloud service resources. Including KMS related operation authority.

○ QcloudAccessForCLSRoleInClsETL
This policy allows CLS(Cloud Log Service) DataTransform task to play a role as the clients themselves to Access their Log Topics in CLS, including push logdata, create logsets、 log topics and log indexes, those...

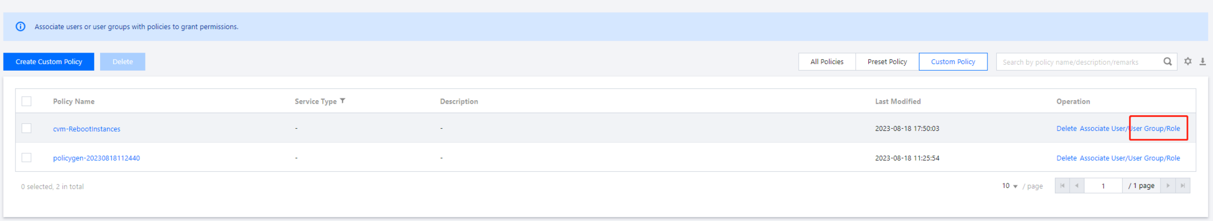
○ QcloudAccessForCLSRoleInTemplate
This policy allows CLS(Cloud Log Service) Template to play a role as the clients themselves to create 、 modify、 describe indexes, shipper tasks from CLS to COS or Ckafka .

4. On the **Edit Policy** page, fill out the following form:
   - Policy name: By default, it is `policygen-current date` . It is recommended that you define a unique and meaningful policy name, such as cvm-RebootInstances.
   - Description: Optional, feel free to compose your own.
   - Policy content: Copy and paste the following content. Here, `test1` is the tag key name, which can be in Chinese or English, and `false` is the fixed tag value.

```
  {
"version": "2.0",
 "statement": [
  {
     "effect": "allow",
     "action": "*",
     "resource": "*",
     "condition": {
        "null_equal": {
           "qcs:resource_tag/test1": "false",
           "qcs:resource_tag/test2": "false",
           "qcs:resource_tag/Owner": "false"
 }
```

```
        }
        }
         ]
        }
```

5. Click **Complete** to finalize the creation of the policy. The new policy will be displayed on the Policy List page.
6. In the Policy List, search for and locate the policy you just created, then click **Associate User/Group/Role** under the operation column on the right.

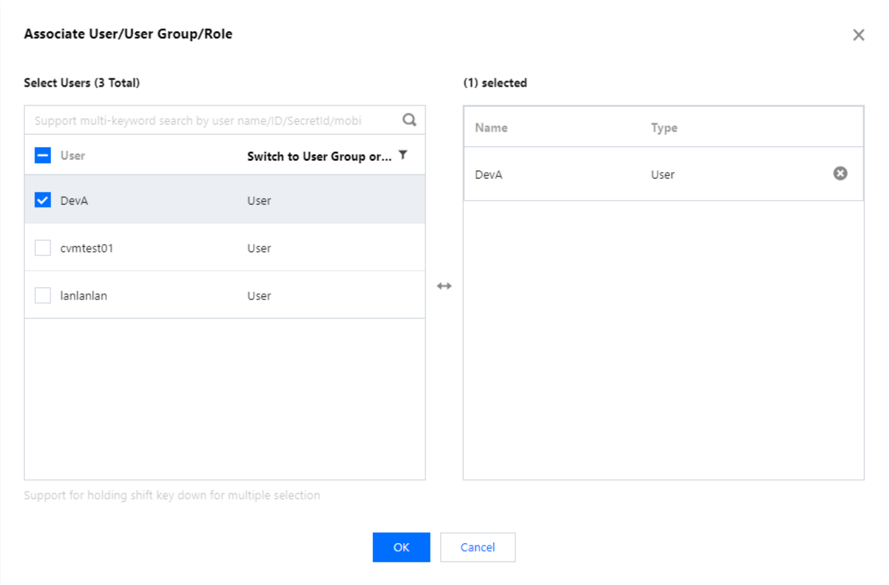


Associate users or user groups with policies to grant permissions.

□	Policy Name	Service Type	Description	Last Modified	Operation
□	cvm-RebootInstances	-	-	2023-08-18 17:50:03	Delete Associate User/User Group/Role
□	policygen-20230818112440	-	-	2023-08-18 11:25:54	Delete Associate User/User Group/Role

0 selected, 2 in total

7. In the "Associate User/User Group" window that pops up, search for and select the sub-account DevA, then click **OK** to complete the authorization process.
   The sub-account DevA will have access to all resources under the tag test1.



Associate User/User Group/Role

Select Users (3 Total)

Support multi-keyword search by user name/ID/SecretId/mobi

	User	Switch to User Group or...
☑	DevA	User
□	cvmtest01	User
□	lanlanlan	User

(1) selected

Name	Type
DevA	User

Support for holding shift key down for multiple selection

Grant a sub-account the authority to bind only to a specific tag key (request_tag)

Scenario

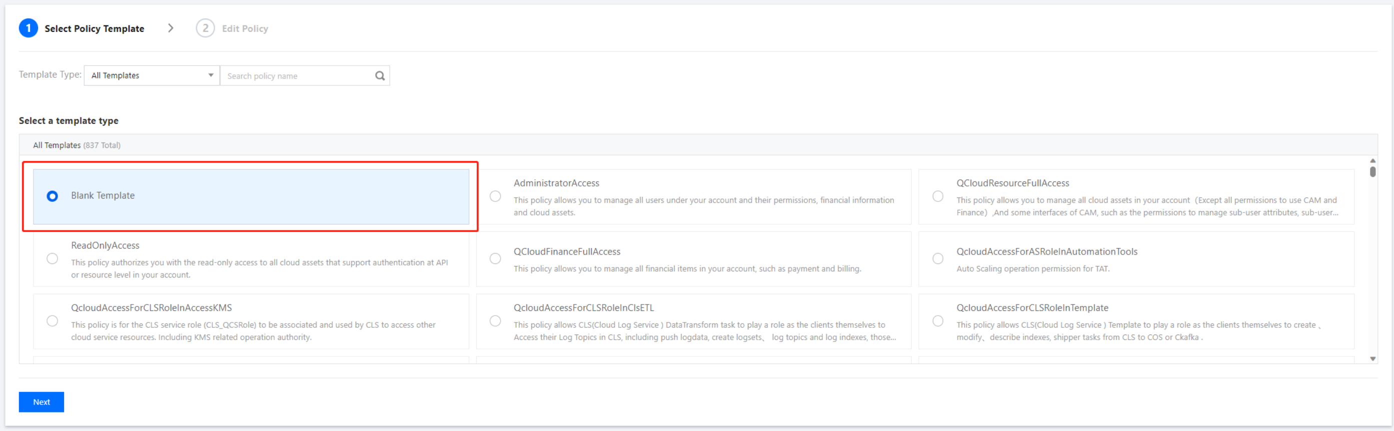
If your company has purchased a variety of Tencent Cloud resources, all managed through tag grouping, you may intend to grant a sub-account the authority to bind only to a specific tag key (request_tag).

Suppose that:

- There is a sub-account, DevA, under the enterprise account CompanyExample.
- The enterprise account, CompanyExample, has a tag key named test1.
- The enterprise account, CompanyExample, intends to grant the sub-account, DevA, the authority to bind only to a specific tag key (request_tag).

Instructions

1. Log in to the Cloud Access Management Console as the enterprise account CompanyExample.
2. On the **Policies** page, click **Create Custom Policy** > **Create by Policy Syntax**.
3. Under the module type selection, choose the blank template and click **Next** to proceed to the policy editing page.



Select a template type

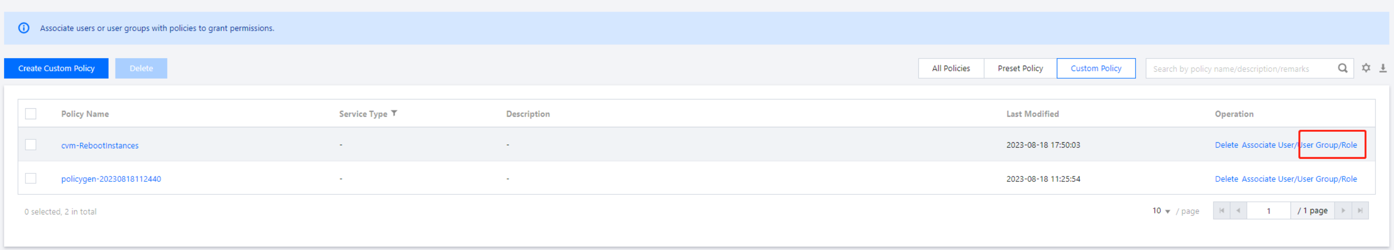
All Templates (837 Total)

- ● Blank Template
- ○ AdministratorAccess — This policy allows you to manage all users under your account and their permissions, financial information and cloud assets.
- ○ QCloudResourceFullAccess — This policy allows you to manage all cloud assets in your account（Except all permissions to use CAM and Finance）,And some interfaces of CAM, such as the permissions to manage sub-user attributes, sub-user...
- ○ ReadOnlyAccess — This policy authorizes you with the read-only access to all cloud assets that support authentication at API or resource level in your account.
- ○ QCloudFinanceFullAccess — This policy allows you to manage all financial items in your account, such as payment and billing.
- ○ QcloudAccessForASRoleInAutomationTools — Auto Scaling operation permission for TAT.
- ○ QcloudAccessForCLSRoleInAccessKMS — This policy is for the CLS service role (CLS_QCSRole) to be associated and used by CLS to access other cloud service resources. Including KMS related operation authority.
- ○ QcloudAccessForCLSRoleInClsETL — This policy allows CLS(Cloud Log Service) DataTransform task to play a role as the clients themselves to Access their Log Topics in CLS, including push logdata, create logsets、 log topics and log indexes, those...
- ○ QcloudAccessForCLSRoleInTemplate — This policy allows CLS(Cloud Log Service) Template to play a role as the clients themselves to create 、modify、describe indexes, shipper tasks from CLS to COS or Ckafka .

4. On the **Edit Policy** page, fill out the following form:
   - Policy name: By default, it is `policygen-current date` . It is recommended that you define a unique and meaningful policy name, such as cvm-RebootInstances.
   - Description: Optional, feel free to compose your own.
   - Policy content: Copy and paste the following content. Here, `test1` is the tag key name, which can be in Chinese or English, and `false` is the fixed tag value.

```
  {
"version": "2.0",
 "statement": [
  {
     "effect": "allow",
     "action": "*",
     "resource": "*",
     "condition": {
       "null_equal": {
         "qcs:request_tag/test1": "false",
         "qcs:request_tag/test2": "false",
         "qcs:request_tag/PersonInCharge": "false"
}
}
}
 ]
}
```

5. Click **Complete** to finalize the creation of the policy. The new policy will be displayed on the Policy List page.
6. In the Policy List, search for and locate the policy you just created, then click **Associate User/User Group/Role** under the operation column on the right.



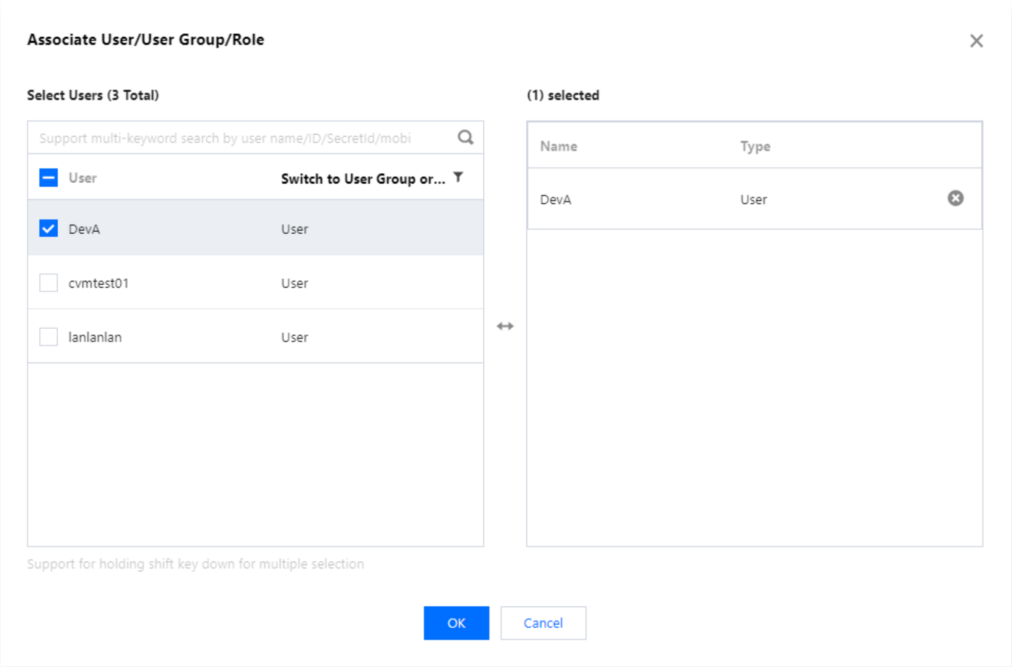
Associate users or user groups with policies to grant permissions.

□	Policy Name	Service Type	Description	Last Modified	Operation
□	cvm-RebootInstances	-	-	2023-08-18 17:50:03	Delete Associate User/User Group/Role
□	policygen-20230818112440	-	-	2023-08-18 11:25:54	Delete Associate User/User Group/Role

0 selected, 2 in total

7. In the "Associate User/User Group/Role" window that pops up, search for and select the sub-account DevA, then click **OK** to complete the authorization process.

The sub-account DevA will have access to all resources under the tag test1.



Associate User/User Group/Role

Select Users (3 Total)

Support multi-keyword search by user name/ID/SecretId/mobi

☐ User	Switch to User Group or...
☑ DevA	User
☐ cvmtest01	User
☐ lanlanlan	User

(1) selected

Name	Type
DevA	User

Support for holding shift key down for multiple selection

Associated Documents

If you intend to understand how to establish a relationship between resources and tags, see Manage Tags .