Cloud Access Management

FAQs

Contents

FAQs
Policy-related Queries

Last updated: 2023-08-31 19:02:42

Why does a new policy version appear in the preset policy?

Preset policies are created and managed by Tencent Cloud, encompassing a collection of commonly used permissions that are frequently accessed by users.
Preset policies are closely related to the functionality of cloud services. If a cloud service undergoes an upgrade or adjustment, Tencent Cloud may correspondingly upgrade or adjust the preset policies. In such cases, a new policy version is added to ensure coverage of the new functional permissions. The preset policies that may be adjusted include general preset policies and those associated with service roles.

How do I grant a sub-account specific operation permissions of specific products?

You can create a custom policy using the Policy Generator, selecting the products and operations you require, and then associate it with the user through Policy Association. Once the association is successful, your sub-account will manage the resources under the main account within the scope of the permissions you have set.

Why do I get a prompt saying that "The account is not on the allowlist" when creating a policy?

Currently, several products are in the beta phase, and some of them do not yet support CAM management. You can check the Products Supported by CAM to determine whether and to what extent you can manage product service permissions in CAM.
If you need to manage a product in beta using CAM, please submit a ticket to proceed.

Why can't a sub-account access certain Tencent Cloud products after it has been authorized with the read-only policy (ReadOnlyAccess)?

- The cloud product read-only policy (ReadOnlyAccess) only includes read interfaces for cloud products authorized at the operation level or resource level. If you access service-level cloud products or write interfaces for operation-level/resource-level cloud products, you will receive a no permission prompt. For the authorization granularity of cloud products, please refer to Products Supported by CAM.
- Please check whether the sub-account's custom policies (user permission policies, permission policies of the user group joined) have set `"effect": "deny"` for the read-only

policy (ReadOnlyAccess). For details, please refer to Scenarios where the "deny" permission policy does not take effect.

What permissions does a sub-account have?

The permissions of a sub-account depend on the policies you bind to it. For more details, refer to the Permissions and Policies documentation.

What permissions are required for a sub-account to purchase cloud products?

- To purchase pay-as-you-go cloud products, it is generally sufficient to assign the sub-account the permission to create instances or resources for that cloud product.
- To purchase annual or monthly cloud products, you need to grant the sub-account additional permissions to pay for orders. This can be done by associating it with the `QCloudResourceFullAccess` policy (a preset policy that allows you to manage all cloud service assets within the account), or by associating it with the `QCloudFinanceFullAccess` policy (a preset policy that allows you to manage finance-related content within the account, such as payments and invoicing) and the permissions to create instances or resources for each cloud product.
- When purchasing certain cloud products, it may be necessary to use or create various other resources. In such cases, the sub-account needs to have the appropriate read or create permissions for these resources.

How do I set payment permissions for a sub-account?

1. Log in to the Cloud Access Management Console with the main account, navigate to **Users** > **User List**, select the corresponding sub-account, and click **Authorize** in the operation column.
2. In the pop-up policy association window, select QCloudResourceFullAccess (a preset policy that allows you to manage all cloud service assets within the account) and click **OK** to complete the payment authorization for the sub-account.

How do I set permissions for a sub-account to view bills?

Sub-accounts do not have standalone permissions to view bills. If needed, you can assign the `QCloudFinanceFullAccess` policy to the user (this policy allows you to manage financial-related content within the account, such as payments and invoicing). For more details, please refer to Authorization Management.

Is it possible to create an account that can only use the ticketing function?

Indeed, you can create a sub-account without granting any permissions.

> **Note**
> The tickets submitted by a sub-account are not visible to the main account; they can only be viewed by logging into that specific sub-account.

Is it possible to set read-only permissions for all products?

Yes, you can do so by granting the ReadOnlyAccess policy.

How should I grant permissions to allow a sub-account to only view part of my resources?

The following example illustrates how to grant a sub-account permission to view a limited list of resources. For more details:
The enterprise account `CompanyExample` (ownerUin: 12345678) has a sub-account `Developer`. `CompanyExample` wants to allow the sub-account to view only part of its resources in the console.
For example, to allow the sub-account to view in the Console two CVM instances whose ID is `ins-xxx1` and `ins-xxx2` in the `gz` region:

1. Create the following policy by using policy syntax:

```
 {
 "version": "2.0",
 "statement": [
 {
 "action": [
 "cvm:DescribeInstances"
 ],
"resource": ["qcs::cvm:gz::instance/ins-xxx1",
 "qcs::cvm:gz::instance/ins-xxx2"
 ],
 "effect": "allow"
}
 ]
}
```

You can also set higher permissions as needed, such as full read/write permissions. If you need full read/write permissions for all cloud server instances in the Guangzhou region, you can write the policy syntax as follows:

```
 {
```

```
  "version": "2.0",
  "statement": [
   {
      "action": [
         "cvm:*"
         ],
      "resource": "qcs::cvm:gz::*",
      "effect": "allow"
}
 ]
}
```

2. Authorize this policy for the sub-account. For the method of authorization, please refer to Authorization Management.
   Currently, the products that **support** read-only operation for resource granularity permission control include: Cloud Virtual Machine (CVM), TencentDB for MySQL, and Tencent Kubernetes Engine (TKE).
   For other products, it is not currently possible to authorize read-only permissions for specific resources. You can only grant the sub-account permission to view all resources, or not view any resources at all.

Why does the "deny" authorization statement in the permission policy not take effect?

When a permission policy contains both "allow" and "deny" authorization statements, it is necessary to determine whether "deny" is effective based on the specific scenario. For details, please refer to Scenarios where permission policy deny is ineffective.

How can I restrict the access permissions of the APPID service?

Currently, in the policies of Access Management, only the resource owners of Object Storage COS and Archive Storage CAS services can be described using the UID method (i.e., APPID), while the resource owners of other services can only be described using the UIN method. For specific usage, please refer to Resource Description Method.
For COS authorization, please refer to Granting a Sub-account All Permissions to a Specific Directory.

Is IP access restriction supported?

Indeed, you can restrict the sub-account's access IP through a custom policy. For specific operations, please refer to IP Access Restrictions.

What should I do if I cannot find the permissions for a specific service?

Possible Cause	Solution
The service requiring permission settings has not been integrated with CAM.	See Business Interfaces that Support CAM to check whether the service has been integrated with CAM.
The service or permission name searched is incorrect.	Based on the product name in Business Interfaces Supported by CAM, search for the corresponding policy permissions on the Cloud Access Management Console > Policies page.

If the problem persists, please submit a ticket to contact us.

User-related Queries

Last updated: 2023-08-31 19:03:07

What are the Types and Differences of CAM Users?

For a detailed explanation, please refer to User Types.

How do I grant permissions to the root account?

The root account inherently possesses all permissions and does not require authorization.

How can a sub-account modify its login password?

- Sub-users: Cannot independently modify the password, the root account or administrator account needs to reset the login password for the sub-user.
- Collaborator: Please refer to Modifying Account Password.

How can a sub-account manage its security settings independently?

The sub-account can request the root account to associate it with the following corresponding policies:

- Self-service management of console login password: Sub-accounts associated with the QcloudCollPasswordManageAccess policy are permitted to manage their console login passwords independently.
- Self-manage API keys: Sub-accounts associated with the QcloudCollApiKeyManageAccess policy are permitted to manage their own API keys.
- Self-service management of MFA devices: Sub-accounts associated with the QcloudCollMFAManageAccess policy are permitted to manage their own MFA devices.

After a sub-account is authorized, which account owns the resources purchased by the sub-account?

Resources purchased by the sub-account are owned by the root account.

How will the fees incurred by resource purchases made by a sub-account be paid?

Fees incurred by the sub-account will be deducted from the balance of the root account.

How to securely create a sub-user?

1. A new sub-user can be created using the root or administrator account. Refer to Creating a Sub-User.

2. Upon successful creation of a user, copy or send the sub-user's username, password, and other information to the designated email to communicate with the sub-user (you can also download all the information of the newly created user).
3. On the sub-user details page, copy the quick login link and send it to the sub-user.
4. Sub-users log in to the console using the received login link, username, and password, and then modify the password.

What should I do if the sub-account login fails?

Error	Solution
"The account does not exist or the password is incorrect. Please re-enter."	Please verify the correctness of your username and password. If you have forgotten your password: • Collaborator: Independently Change Account Password. • Sub-users: Contact the root account to Reset Password.
"Temporarily unable to log in"	Follow the prompts to send a temporary access request, or ask the administrator to cancel the login restrictions.

How can one regulate a sub-account's access to the console?

You can enable abnormal login restrictions (logins from unusual locations, no logins for 30 days) and IP login restrictions (specifying IPs allowed or not allowed to log in) for sub-accounts to ensure they log in to the Tencent Cloud console in a secure environment. For detailed operations, please refer to Login Restrictions.

How do I activate login protection and operation protection?

Refer to Identity Security Management to enable "Virtual MFA Device Verification" for the sub-account.

How do I disable login protection?

Refer to Identity Security Management and set the login protection to "Disabled".

How do I disable operation protection?

Refer to Identity Security Management and set the operation protection to "Disable".

How do I bind a Virtual MFA Device?

For related settings, please refer to: Setting Security Protection for Collaborators, Setting Security Protection for Sub-users.

How can I view the sub-account's password through the root account?

Access Management does not currently support viewing a sub-account's password through the root account; it can only be reset by the root account. For detailed instructions, please refer to Resetting the Login Password for Sub-users.

How can a sub-account alter its email address and phone number?

Ordinary sub-accounts cannot modify information such as mobile phone numbers and email addresses. These changes need to be made by the root account or administrator account in the **User Details** section of the **Cloud Access Management Console > User List**.

Can WeCom sub-users be automatically synced to CAM?

Currently, auto-sync is not supported for WeCom sub-users.

Does the sub-user support WeChat login?

Indeed. After logging into the sub-account, navigate to Account Information to bind WeChat. The next time you log in, you can simply scan with WeChat.

Role-related Queries

Last updated: 2023-08-31 19:06:54

Why are there new roles in my account?

When you perform a specific operation (such as authorizing the creation of a service role) for a Tencent Cloud service, the service will send you a request for the authorization. After you indicate your consent, a service role will be automatically created and be associated with related policies.
If you have been using a service before it started supporting service-related roles, a new role will be automatically created in your account once you have been notified via email or other means.

Has the policy associated with the service role changed?

After a Tencent Cloud service is authorized to create a service role and grant permissions to it, the service feature may be upgraded. During the upgrade, the permission to call other Tencent Cloud service APIs may be added.
To ensure you can enjoy complete Tencent Cloud service features, we will associate new policies with the created service role or add new API permissions to the policy associated with the service role.
This change only applies to the Tencent Cloud services you are using and won't affect the authorization for other sub-users.

How can I view the RoleArn of a role?

Navigate to the Role Console, click on the name of the role you wish to query. This will take you to the role details page where you can find the information in the role information section.

How many types of CAM roles are there?

There are three types of CAM roles based on different role entities:

- **Tencent Cloud Product Service**: Authorize Tencent Cloud service to utilize your cloud resources via roles.
- **Tencent Cloud Account**: Authorize the root account or other root accounts to use your cloud resources via roles.
- **Identity Provider**: Authorizes external Tencent Cloud user identities (such as corporate user directories) to utilize your cloud resources.

Key-related Queries

Last updated: 2023-08-31 19:08:41

What is an API key?

An API key is an important identity credential for making Tencent Cloud API requests. You can use APIs to manage resources under your Tencent Cloud account. For the security of your assets and services, store your keys safely and change them regularly.

Where can I view the API key?

The API key, also known as the access key, can be viewed in different places depending on the account type. For the primary account, please refer to Main Account Access Key. For sub-accounts, please refer to Sub-user/Collaborator Access Key.

How do I authorize a sub-account key?

The sub-account key shares the same permissions as the sub-account. By granting permissions to the sub-account, the sub-account key will automatically have the corresponding permissions. For setting sub-account permissions, please refer to Setting Sub-user Permissions.

How can I determine if the API key is still in use?

You can determine whether an API key is still in use by checking the last usage time of the access key through the Cloud Access Management Console or API interface. The specifics are as follows:

View Channel	Viewing Method
Cloud Access Management Console	• The root or sub-account can log in to **Cloud Access Management Console > Access Key** to view the last usage time of the API key for that account. • The root account or a sub-account with administrative permissions can log in to **Cloud Access Management Console > User List**. In the **User Details** > **API Key** section, you can view the last time the sub-account's API key was used (refer to Viewing Sub-account Key).
Related APIs	Invoke the SecretIdLastUsedRows interface to view the last usage time of the primary or sub-account API key.

Can an API key be recovered after deletion?

Irretrievable. Once an API key is deleted, Tencent Cloud will permanently reject all requests from this key.

Is there a limit to the number of API keys that can be created in CAM?

A primary or sub-account can create up to two API keys. For more information, please refer to Main Account Access Key Management and Sub-account Access Key Management.